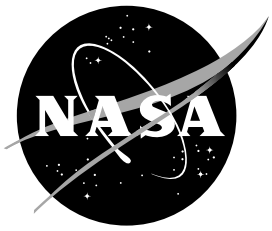


National Aeronautics and Space Administration
Ames Research Center
Moffett Field, California 94035

NASA Operational Certification Authority (NOCA)
Registration Practice Statement

March 30, 2007
Revision 1.0

National Aeronautics and Space Administration
Ames Research Center
Moffett Field, CA. 94035-1000

NASA Operational Certification Authority Registration Practice Statement

Signature:

_____ _____

Date

DOCUMENT HISTORY LOG

Revision	Description of Change	Written By	Date
0.1	Initial document for review by NASA and Treasury	Helen Euler	1/31/07
0.2	Revised with Treasury BPD comments	Helen Euler	2/22/07
1.0	Final document with PKI TWG comments	Helen Euler	3/30/07

NASA Operational Certification Authority Registration Practice Statement

Table of Contents

1. INTRODUCTION 1

1.1 OVERVIEW 1
1.1.1 Responsibilities 2
1.1.2 NASA PKI Structure 2
1.2 IDENTIFICATION 5
1.3 COMMUNITY & APPLICABILITY 6
1.3.1 Policy and Certification Authorities (CAs) Community and Applicability 6
1.3.2 NOCA Community and Applicability 7
1.3.3 Applicability 10
1.3.4 Suitable Applications 10
1.4 CONTACT DETAILS 10

2. GENERAL PROVISIONS 11

2.1 OBLIGATIONS 11
2.1.1 Trusted Operations 11
2.1.2 Certificate Issuance Liability 12
2.1.3 Trusted Administration 12
2.1.4 End Entities 13
2.1.5 Repository Obligations 15
2.2 LIABILITY 15
2.2.1 CA Liability 15
2.2.2 RA Liability 16
2.2.3 Subscriber Liability 16
2.2.4 Relying Party Liability 16
2.3 FINANCIAL RESPONSIBILITY 16
2.4 INTERPRETATION AND ENFORCEMENT 16
2.4.1 Governing Law 16
2.4.2 Jurisdiction 17
2.4.3 Severability, Survival, Merger, Notice 17
2.4.4 Dispute Resolution Procedures 17
2.5 FEES 17
2.6 PUBLICATION & REPOSITORY 17
2.6.1 Publication of CA Information 17
2.6.2 Frequency Of Publication 17
2.6.3 Access Controls 18
2.6.4 Repositories 18
2.7 COMPLIANCE AUDIT 18
2.7.1 Frequency Of Compliance Audit 18
2.7.2 Identity/Qualifications of Auditor 18
2.7.3 Auditor's Relationship to Audited Party 18
2.7.4 Topics Covered by Audit 18
2.7.5 Actions Taken as a Result of Deficiency 19
2.7.6 Communication of Results 19
2.8 CONFIDENTIALITY OF INFORMATION 19
2.8.1 Types Of Information To Be Kept Confidential 19
2.8.2 Types Of Information Not Considered Confidential 19
2.8.3 Disclosure Of Certificate Revocation Information 20
2.8.4 Release to Law Enforcement Officials 20
2.8.5 Release As Part Of Civil Discovery 20

2.8.6 Disclosure Upon Subscriber's Request *20*
2.8.7 Other Information Release Circumstances *20*
2.9 INTELLECTUAL PROPERTY RIGHTS 21
2.9.1 General *21*
2.9.2 Certificates and OIDs *21*
2.9.3 Private Keys *21*

3. IDENTIFICATION & AUTHENTICATION 22

3.1 INITIAL REGISTRATION 22
3.1.1 Types Of Names *22*
3.1.2 Need For Names To Be Meaningful *23*
3.1.3 Rules For Interpreting Various Name Forms *23*
3.1.4 Uniqueness Of Names *23*
3.1.5 Name Claim Dispute Resolution Procedure *23*
3.1.6 Recognition, Authentication And Roles Of Trademarks *24*
3.1.7 Method To Prove Possession Of Private Key *24*
3.1.8 Authentication Of Organization Identity *24*
3.1.9 Authentication Of Individual Identity *25*
3.1.10 Authentication Of Devices Or Applications *28*
3.2 AUTHENTICATION FOR CERTIFICATE RENEWAL, UPDATE AND ROUTINE REKEY 29
3.2.1 Certificate Renewal *29*
3.2.2 Certificate Re-Key *30*
3.2.3 Certificate Update *30*
3.3 AUTHENTICATION FOR REKEY AFTER REVOCATION 31
3.4 AUTHENTICATION OF REVOCATION REQUEST 31

4. OPERATIONAL REQUIREMENTS 32

4.1 APPLICATION FOR A CERTIFICATE 32
4.2 CERTIFICATE ISSUANCE 33
4.2.1 Delivery of Public Key for Certificate Issuance *34*
4.2.2 Delivery of Subscriber's Private Key to Subscriber *34*
4.2.3 CA Public Key Delivery to Subscribers *35*
4.3 CERTIFICATE ACCEPTANCE 35
4.4 CERTIFICATE SUSPENSION & REVOCATION 35
4.4.1 Circumstances For Revocation *35*
4.4.2 Who Can Request Revocation *36*
4.4.3 Procedure For Revocation Request *36*
4.4.4 Revocation Request Grace Period *38*
4.4.5 Circumstances For Suspension *38*
4.4.6 Who Can Request Suspension *38*
4.4.7 Procedure For Suspension Request *38*
4.4.8 Limits On Suspension Period *40*
4.4.9 CRL Issuance Frequency *40*
4.4.10 CRL Checking Requirements *40*
4.4.11 On-line Revocation/status Checking Availability *40*
4.4.12 On-line Revocation Checking Requirements *40*
4.4.13 Other Forms Of Revocation Advertisements Available *40*
4.4.14 Checking Requirements For Other Forms Of Revocation Advertisements *40*
4.4.15 Special Requirements Related To Key Compromise *41*
4.5 SYSTEM SECURITY AUDIT PROCEDURES 41
4.5.1 RA And CA Officer Logbooks *41*
4.6 RECORDS ARCHIVAL 41
4.6.1 Types Of Data Retained *41*
4.6.2 Retention Period for Archive *43*
4.6.3 Protection Of Archive *43*
4.6.4 Archive Backup Procedures *43*

4.6.5 Requirements for Time-Stamping of Records *43*
4.6.6 Archive Collection System *44*
4.6.7 Procedures To Obtain And Verify Archive Information *44*
4.7 KEY CHANGEOVER 44
4.7.1 CA Key Changeover *44*
4.7.2 Subscriber Key Changeover *44*
4.8 COMPROMISE AND DISASTER RECOVERY 45
4.8.1 Computing Resources, Software, and/or Data Are Corrupted *45*
4.8.2 Public Key is Revoked *49*
4.8.3 CA Private Key Compromise *49*
4.8.4 CA Private Key Loss *49*
4.8.5 Secure Facility After a Natural or Other Type of Disaster *50*
4.8.6 CA Cannot Generate CRLs *50*
4.9 CA TERMINATION 50

5. PHYSICAL, PROCEDURAL & PERSONNEL SECURITY 52

5.1 PHYSICAL CONTROLS 52
5.2 PROCEDURAL CONTROLS 52
5.2.1 Trusted Roles *52*
5.2.2 Separation of Roles *54*
5.2.3 Number of Persons Required Per Task *54*
5.2.4 Identification and Authentication for Each Role *55*
5.3 PERSONNEL SECURITY CONTROLS 55
5.3.1 Background, Qualifications, Experience, and Clearance Requirements *55*
5.3.2 Background Check Procedures *56*
5.3.3 Training Requirements *56*
5.3.4 Retraining Frequency And Requirements *57*
5.3.5 Sanctions for Unauthorized Actions *57*
5.3.6 Contracting Personnel Requirements *57*
5.3.7 Documentation Supplied to Personnel *57*

6. TECHNICAL SECURITY CONTROLS 59

6.1 KEY PAIR GENERATION AND INSTALLATION 59
6.1.1 Key Pair Generation *59*
6.1.2 Private Key Delivery To Entity *59*
6.1.3 Public Key Delivery To Certificate Issuer *60*
6.1.4 CA Public Key Delivery To Users *60*
6.1.5 Asymmetric Key Sizes *61*
6.1.6 Public Key Parameters Generation *62*
6.1.7 Parameter Quality Checking *62*
6.1.8 Hardware/software Key Generation *63*
6.1.9 Key Usage Purposes (as per X.509v3 key usage field) *63*
6.2 PRIVATE KEY PROTECTION 63
6.2.1 Standards For Cryptographic- module *64*
6.2.2 Private Key (m of n) Multi-person Control *64*
6.2.3 Private Key Escrow *64*
6.2.4 Private Key Backup *64*
6.2.5 Private Key Archival *65*
6.2.6 Private Key Entry Into Cryptographic Module *65*
6.2.7 Method Of Activating Private Key *65*
6.2.8 Method Of Deactivating Private Key *66*
6.2.9 Method Of Destroying Private Key *66*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 66
6.3.1 Public Key Archival *67*
6.3.2 Usage Periods For The Public And Private Keys *67*
6.4 ACTIVATION DATA 67

6.4.1 Activation Data Generation And Installation *67*
6.4.2 Other Aspects Of Activation Data *67*
6.5 COMPUTER SECURITY CONTROLS 68
6.6 LIFE CYCLE TECHNICAL CONTROLS 68
6.6.1 Certificate Definition Change Procedures *69*
6.7 SECURITY MANAGEMENT CONTROLS 70
6.8 NETWORK SECURITY CONTROLS 70
6.9 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 70

7. CERTIFICATE & CRL PROFILES 71

7.1 CERTIFICATE PROFILE 71
7.1.1 Version Number(s) *71*
7.1.2 Certificate Extensions *71*
7.1.3 Algorithm Object Identifiers *71*
7.1.4 Name Forms *72*
7.1.5 Name Constraints *72*
7.1.6 Certificate Policy Object Identifier *72*
7.1.7 Processing Semantics For The Critical Certificate Policy *73*
7.1.8 Policy Qualifiers Syntax And Semantics *73*
7.1.9 Key Usage Constraints for id-fpki-common-authentication *73*
7.2 CRL PROFILE 73
7.2.1 Version Number(s) *73*
7.2.2 CRL and CRL Entry Extensions *73*
7.3 CERTIFICATE TYPE DEFINITIONS 74
7.3.1 Enterprise Certificates *74*
7.3.2 Web Certificates *75*

8. SPECIFICATION ADMINISTRATION 77

8.1 CHANGE PROCEDURES 77
8.1.1 RPS Change Procedures *77*
8.1.2 CPS Change Procedure *77*
8.2 PUBLICATION AND NOTIFICATION POLICIES 78
8.3 CPS APPROVAL PROCEDURES 78
8.4 WAIVERS 78

APPENDIX A: ACRONYMS 79

APPENDIX B: NASA IDENTITY VERIFICATION 80

APPENDIX C: NASA PIV-I AND NOCA CPS IDENTITY VERIFICATION PROCESSES 89

APPENDIX D: UNSWORN DECLARATION 92

APPENDIX E: DEFINITIONS 93

REFERENCES 97

1. Introduction

The National Aeronautics and Space Administration (NASA) entered into an Agreement with the US Treasury to have the US Treasury as the Shared Service Provider (SSP) for the operation of the NASA Certification Authority (CA), referred to as the NASA Operational Certification Authority (NOCA). Under this Agreement, NASA retains responsibility for the operation of the Registration Authorities (RAs). This document describes the practices for the Registration Authorities that operate under the NOCA. This document's focus is on the responsibilities and procedures for the RAs and is just a component of the overall PKI policies and procedures.

This document assumes an understanding of Public Key Infrastructure (PKI) concepts and technology and a familiarity with NASA PKI. This document is designed for RA personnel and organizations that operate an RA. This document uses the same format as a Certification Practice Statement (CPS) but includes only those sections that apply to RAs and provides more information on RA operation and procedures. This document focuses on RA policies and procedures, for information on operation of the RA software, consult the RA Manual.

As a Registration Practice Statement (RPS), this document has been drafted to comply with the requirements of the Department of the Treasury Public Key Infrastructure NOCA Certification Practice Statement.

Please note, definitions of terms used in this RPS are provided in Appendix E.

To obtain information concerning the underlying policies for this RPS, please consult the “X.509 Certificate Policy for the US Treasury PKI”.

1.1 OVERVIEW

As constituted under SSP environment, the NASA PKI consists of the following components: The NASA PKI consists of

- A central CA, operated by the US Treasury
- RAs at each of the eleven NASA centers operated by NASA personnel
- A central PKI Directory operated by NASA
- Documents that define the policy and procedures:
  - *"Department of the Treasury Public Key Infrastructure NOCA Certification Practice Statement" Version 1.4 dated May 17,2006*
  - *“X.509 Certificate Policy for the US Treasury PKI” Version 1.4 dated August 29, 2002.*
  - *“X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework” Version 2.3 dated September 19 2005.*

This RPS provides policies and procedures that support medium level assurance, unless specified otherwise. As NASA adds other assurance levels, this RPS will be modified to describe the policies for these levels. Please note that the term, “assurance”, refers to the level of trust associated with a certificate.

1.1.1 Responsibilities

As the Shared Service Provider (SSP), The U.S. Treasury, Bureau of Public Debt (BPD) is responsible for the following areas:

- Operation of the NASA CA, NOCA
- Creation and maintenance of the CA Certification Practice Statement
- Oversight of the CA Policy
- Work with the Federal Identity Credentialing Committee (FICC), the Federal Public Key Infrastructure Policy Authority (FPKIPA), and NASA to provide for compliance audits, as provided for in the Federal Common Policy.

As the Contracting Federal Agency, NASA is responsible for the following areas:

- Maintenance of the CA and RA component software
- Maintenance of the Subscriber and Server PKI software
- Operation of the PKI Directory the RA function
- Identification and management of the authoritative data source used to create digital credentials
- Management, operational and technical controls over the RA, in compliance with the Federal Common Policy, the Department of Treasury PKI NOCA CPS, and this Registration Practice Statement (RPS)
    - Includes any delegated RA functions such as a Trusted Agent or Trusted Registration Authority (TRA)

1.1.2 NASA PKI Structure

There are several entities that make up the NASA PKI Structure. Provided below is a brief description of these entities with more detailed information provided in Section 1.3.

The Policy Management Authority (PMA) is responsible for the overall management of the NOCA. The PMA is responsible for defining the policies under which NOCA operates. The PMA duties include ensuring that the NOCA operates in accordance with policies and practices defined in relevant Certification and Certificate documents, and approving and administering any modifications to these documents identification of applicable object identifiers (OIDs) will be

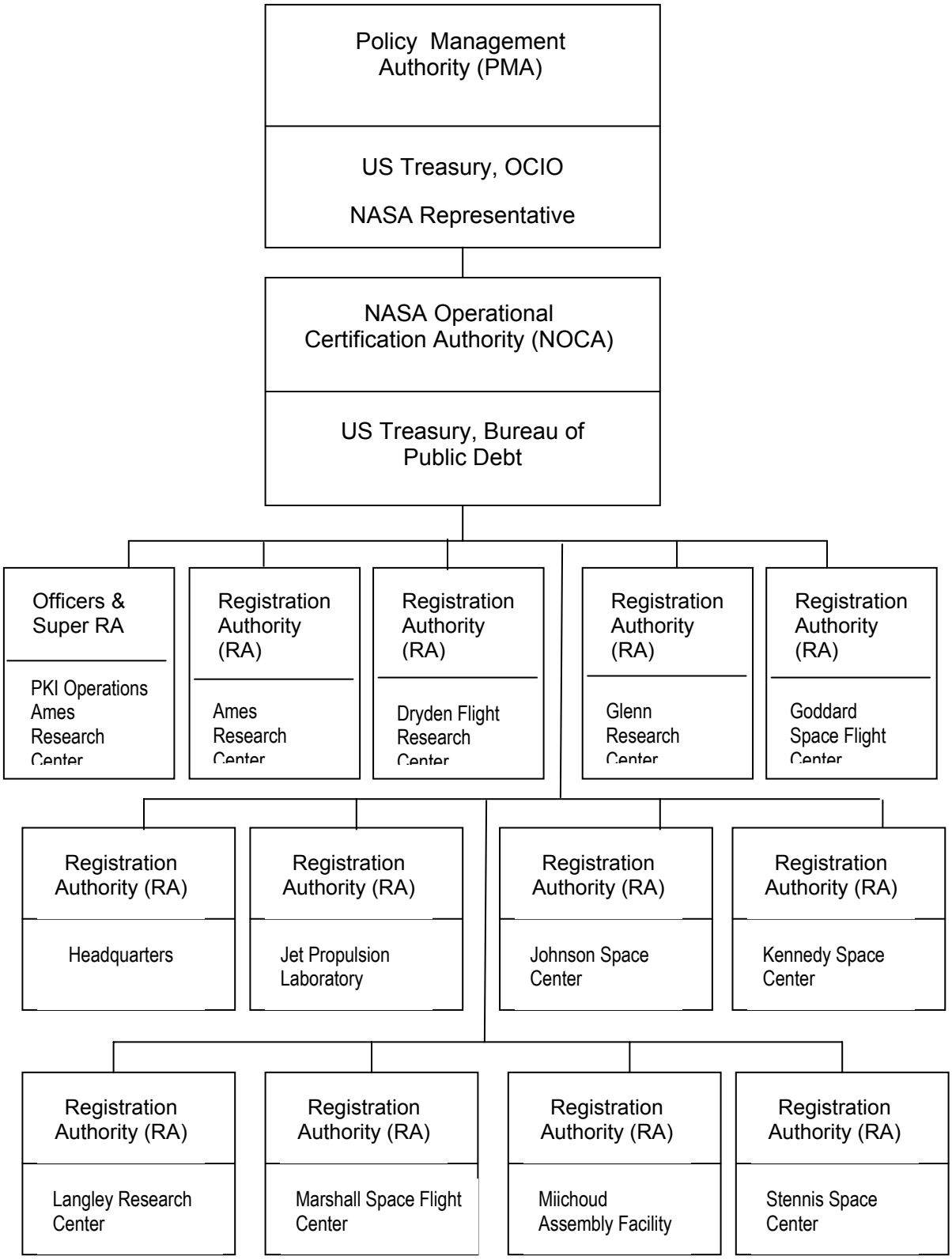
included in NASA certificates. The PMA is vested in the US Treasury, Office of the Chief Information Officer (OCIO). NASA has a representative that participates in the PMA meetings.

The NOCA is responsible for the creation and management of Version 3 X.509 public-key certificates for use by NASA and in accordance with the Department of Treasury PKI NOCA CPS. As noted earlier, the US Treasury Bureau of Public Debt operates the NOCA.

NASA uses Registration Authorities (RAs) to collect information, verify identity and authorize, and request certificate management actions on behalf of their Subscriber population. There are twelve operating Registration Authorities.

The diagram on the following page depicts the general structure of the NASA PKI.

NASA PKI STRUCTURE



1.2 IDENTIFICATION

Object identifiers (OIDs) will be included in NASA certificates. In the area of level of assurance, OIDs will be used to indicate the level of assurance associated with a certificate. Certificates supported in this RPS and issued in accordance with the Department of Treasury PKI NOCA CPS will assert at least one of the following OID combinations in the certificate policy extension in the table below.

These policy assertions are due to the subordinate relationship to the Common Policy Root CA and the US Treasury Root CA. The table also defines display names, which will be referred to throughout the remainder of this RPS.

Assurance Level	Object Identifiers
Medium (Software)	id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
Medium (Hardware)	id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7} treasury-policies-medium ::= {2 16 840 1 101 3 2 1 5 4}
Device	id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8} treasury-policies-medium ::= {2 16 840 1 101 3 2 1 5 4}
Authentication	id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13} treasury-policies-medium ::= {2 16 840 1 101 3 2 1 5 4}

Certificates issued to users to support digitally signed documents or key management will contain the OID(s) for Medium (Software). The Medium Software OID pertains to the NASA certificates issued to Subscribers for encryption and digital signature with the keys and certificates issued in software.

The Medium (Hardware) OID pertains to NASA certificates issued to Subscribers for encryption and digital signature with keys and certificates issued in a hardware token or Smart Card. At the time of this RPS publication, NASA has not determined if encryption or signing certificates will be included in the NASA Smart Card, therefore reference to Medium (Hardware) OIDs is informational only.

Certificates issued to devices will contain the OID(s) for Device.

Certificates issued to users supporting authentication will contain the OID(s) for Authentication. These certificates will be used in the NASA Smart Card implementation.

1.3 COMMUNITY & APPLICABILITY

1.3.1 Policy and Certification Authorities (CAs) Community and Applicability

1.3.1.1 TREASURY PROGRAM MANAGEMENT OFFICE (PMO)

The Treasury PMO is the Office of the Assistant Director for eGovernment Operations, Customer Service Infrastructure Operations (CSIO), and Office of the Chief Information Officer. The PMO is responsible for:

- Review and approval of the Certificate Policy (CP) and all CPSs pertaining to the Treasury PKI with the exception of the Treasury Root CPS which is under the domain of the Treasury PMA
- Acceptance of applications from Bureaus and Offices for certification of their subordinate CAs within the Treasury PKI
- Treasury RA Training
- Treasury RA guidance
- Determination regarding CPS compliance and assurance level with the Treasury CP

1.3.1.2 TREASURY POLICY MANAGEMENT AUTHORITY (PMA)

The Policy Authority for the NOCA is the Treasury Policy Management Authority (PMA). The PMA is responsible for:

- Review and approval of all Treasury PKI Policy
- Review and approval of all Treasury CPSs
- Role of Internal Auditor for all Treasury PKI auditable events or operations
- Perform internal compliance audits and review of Treasury PKI operations
- Review and approval of any CPS for CA's subordinate to the Treasury Root CA
- Responsible for authenticating a subordinate CA, along with its CP and CPS

NASA has representative on the Treasury PMA to attend all PMA meetings and present NASA policy requirements.

1.3.1.3 TREASURY ROOT CERTIFICATION AUTHORITY (TRCA)

The Treasury Root Certification Authority (TRCA) signs all subordinate CA certificates adhering to the Treasury X.509 Certificate policy, including the NOCA. It is also responsible for revocation of its subordinate CAs.

1.3.1.4 NASA OPERATIONAL CERTIFICATION AUTHORITY (NOCA)

The NOCA is the collection of hardware and software and trusted roles used to issue certificates to Subscribers. The Treasury CP and the CPS are all binding on the NOCA and govern its performance with respect to all certificates that it issues. The NOCA is responsible for the following, but not limited to:

- Certificate creation
- Certificate signing
- Certificate revocation
- Key management
- Publication of certificate revocation lists (CRLs) and authority revocation lists (ARLs)

1.3.2 NOCA Community and Applicability

There are three distinct entity categories within the NOCA community. As shown here, each category includes several roles. The roles within each category are described in the following sections:

Trusted Operations

- Certification Authority (NOCA)
- CA Issuer
- CA Repository
- Security Officer (SO)
- Registration Authority (RA)

Trusted Administration

- NOCA Administrators
- Operators
- Directory Administrators
- Auditors
- Trusted Registration Agents (TRAs)

End Entities

- Applicants
- Subscribers

- Relying Parties
- PKI Sponsors

1.3.2.1 TRUSTED OPERATIONS

1.3.2.1.1 Certification Authority

The Department of the Treasury, Bureau of the Public Debt (BPD), operates the NOCA. The NOCA provides public key certificate services (e.g., the CA is the authority that issues and manages public key certificates and CRLs). The NOCA is referred to throughout this RPS as the CA system. The CA system is an entity of combined Trusted Operations and Trusted Administration.

1.3.2.1.2 CA Issuer

The Issuer is the NOCA (e.g. the name of the CA is embedded in every certificate that the NOCA signs).

1.3.2.1.3 CA Repository

The NOCA Repository contains Certificates, Certificate Revocation Lists (CRLs). The Repository is a Lightweight Directory Access Protocol (LDAP) speaking directory service. This LDAP speaking directory contains certificates and CRLs.

The NOCA also makes use of an HTTP repository for CA and revocation information. This repository is located at the following URL: http://hc.nasa.gov/

1.3.2.1.4 Security Officer

The Security Officer (SO) creates and maintains the security policy, roles, and other applicable information that is used within the NOCA to control operations. NASA PKI personnel perform this function.

1.3.2.1.5 Registration Authorities

The Registration Authorities (RAs) collect and verify each applicant's identity and information that are to be entered into his or her public key certificate. NASA personnel or their contractor performs this function.

1.3.2.2 TRUSTED ADMINISTRATION

Trusted Administration refers to those entities that do not have the ability to issue certificates, but provide an administrative role for the NOCA. Trusted Administration provides control and responsibility for administrative tasks related to the NOCA, and thus require a high level of trust.

These Trusted Administration functions are divided into functions performed by the Department of the Treasury, Bureau of the Public Debt (BPD) Personnel and NASA Personnel.

1.3.2.2.1 BPD Functions

The following functions are performed by the Bureau of Public Debt (BPD):

- CA Administrators
    - CA Administrators are responsible for the operation and maintenance of the NOCA systems and technical infrastructure.

- Operators
    - Operators are similar to the CA Administrators above, but are only responsible for the performance of system backups of the operating system.

- Auditors
    - Auditors work on behalf of the PMA on all auditing matters.

1.3.2.2.2 NASA Functions

The following functions are performed by NASA personnel or their contractor or a trusted agent:

- Directory Administrators
    - Directory Administrators maintain the repository that houses the certificates and Certificate Revocation Lists (CRLs). This includes, but is not limited to, creating and maintaining the directory information tree structure, providing operational backup and, completing directory recovery tasks, etc.

- Trusted Registration Agents
    - Trusted Registration Agents (TRAs) are individuals charged with evaluating, approving, or rejecting certificate applications on behalf of the NOCA. The TRA acts solely as a registrar to physically vet the Applicant in a face-to-face meeting, attaining the Applicant's identification and vouching for the Applicant's requirement to be issued a certificate.

    - A TRA has the ability to provide the Applicant with the means to locally create their credential. However, at no time can the TRA communicate directly with the NOCA. The TRA may not vet any Trusted Operations roles nor may they vet any other TRAs.

    - An example function of the TRA is to allow a Federal Program Agency (FPA) the ability to provide services to its local community without the need for each individual Applicant or Subscriber to travel to a RA facility to be proofed in-person.

1.3.2.3 END ENTITIES

End entities include hardware, software, and people that have a need to use public key infrastructure services from the Service. End Entity types include:

- Applicants

- An Applicant is a potential user of a NOCA issued certificate (e.g., an Applicant applies for a certificate).

- Subscribers
  - Subscribers of the NOCA consist of the human users and non-human system components. The human subscribers consist of authorized public and private sector personnel, e.g., business customers, as well as NASA employees. The non-human system components consist of NASA computers and other devices that require public key certificates.

- Relying Parties
  - Relying Parties consist of any human, device, or process that places any amount of trust in a certificate or CRL issued by the NOCA.

- PKI Sponsor
  - A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects.

1.3.3 Applicability

This RPS applies to all certificates issued by the NOCA. The NOCA offers services to identify and map a public key to a user, device, or application. The NOCA does not provide services to a private entity for the purposes of individual use.

The practices described in this RPS apply to the NOCA and its administrators, the NASA RAs and their administrators, the repository used by the NOCA.

1.3.4 Suitable Applications

The sensitivity of the information processed or protected using certificates issued by the NOCA are up to and including Sensitive Unclassified.

1.4 CONTACT DETAILS

This RPS is administered by the NASA PKI Operations, Applied Information Technology Division, Ames Research Center. The address is:

NASA PKI Operations
Applied Information Technology Division
MS: 233-10
Ames Research Center
Moffett Field, CA 94035-1000

2. General Provisions

2.1 OBLIGATIONS

2.1.1 Trusted Operations

The NOCA refers to a logical organization of Trusted Operations and Trusted Administration, as well as the CA system(s) and other supporting systems operated by the Bureau of the Public Debt. The Issuer refers to the Issuer attribute embedded in every certificate it signs. Due to these definitions of parties, there are no specific obligations assigned to the NOCA, nor the Issuer.

2.1.1.1 NOCA REPOSITORY OBLIGATIONS

Maintain availability of the information as required by section 2.6 of this RPS.

2.1.1.2 SECURITY OFFICER OBLIGATIONS AND CA OBLIGATIONS

The Security Officer(s) has the following obligations:

a. Work with the Directory Administrator to ensure that there is no collision of the Subscriber's name, as defined in the Distinguished Name (DN) on the Subscriber's certificate, with that of any other Subscriber within the NOCA Domain;

b. Designate all policy settings and the number of authorizations for sensitive operations for the NOCA Administration software in accordance with the NOCA CPS and this RPS;

c. Act as substitute RAs when RA is not available or in emergency situations;

d. Perform key recovery for RAs, when RA role requires a key recovery;

e. Add or delete RAs or other Security Officers.

The NOCA itself is composed of software that provides services and it is through the system configuration and policy settings designated by the Security Officer that the NOCA has the following obligations:

a. Issue, and make available, certificates within a reasonable time after receipt of a properly formatted and validated certificate request;

b. Provide to the RA the Activation Data generated for the Subscriber;

c. Publish all certificates and certificate status information to the Repository.

2.1.1.3 REGISTRATION AUTHORITIES OBLIGATIONS

The RA(s) have the following obligations:

a. Verifying the identity of Applicants and the accuracy of information to be included in the Subscriber certificate;

b. Coordinate and update assignment information as events warrant (due to employee reassignment, termination, etc.);

c. Process incoming applications for certificates;

d. Approve and forward the application to the Security Officer after successfully verifying the identity of the Applicant);

e. Notify the NOCA of the date when a Subscriber's certificate will be revoked.

2.1.2 Certificate Issuance Liability

The United States Government disclaims any liability that may arise from use of any certificate issued by the NOCA, or the NOCA determination to revoke a certificate issued by the NOCA. In no event will the U.S. Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the NOCA.

2.1.3 Trusted Administration

2.1.3.1 NOCA ADMINISTRATORS OBLIGATIONS

The NOCA Administrators are obligated to maintain the NOCA systems and technical infrastructure, which includes:

a. Perform backups and recovery for the NOCA Software, data, and logs;

b. Protection of the NOCA signature key;

c. Monitoring of the NOCA software application platform and reporting of non-working services;

d. Performance of the operation and maintenance of the NOCA hardware and operating system;

e. Execution of scripts and routines that manage operating system log creation and deletion on the NOCA systems;

f. Initiating change control procedures for the operating system to perform upgrades or install patches.

2.1.3.2 OPERATORS OBLIGATIONS

Operators are obligated to:

a. Perform backups of the NOCA server's operating systems;

b. Perform backups of the NOCA server's operating systems logs.

2.1.3.3 DIRECTORY ADMINISTRATORS OBLIGATIONS

Directory Administrators are obligated to:

a. Ensure timely publication of NOCA information to the Repository, and;

b. Provide access control mechanisms sufficient to protect Repository information.

2.1.3.4 AUDITORS OBLIGATIONS

Auditors are responsible for:

a. Arranging and overseeing external compliance audits to ensure that the NOCA is operating in accordance with its CPS;

b. Performing or overseeing internal compliance audits to ensure that the NOCA is operating in accordance with its CPS.

2.1.3.5 TRUSTED REGISTRATION AGENTS OBLIGATIONS

The TRAs, has the following obligations:

a. Identify in writing to the RA(s), the TRAs names and contact information

b. Update the information as events warrant (due to employee reassignment, termination, etc.)

c. Notify the RA(s), if the Subscriber:
   1. Is no longer employed or affiliated with the TRA organization;
   2. No longer requires its private key;
   3. Has reason to believe that its private key has been compromised, or;
   4. No longer has access to its private key (Ex: Can not remember password that unlocks private key)

2.1.4 End Entities

2.1.4.1 APPLICANTS OBLIGATIONS

An Applicant has the following obligations:

a. Provide accurate information as part of the certificate application process;

b. Provide password protection of the private key if the key pair is generated before the Applicant's identity is verified;

c. Destroy the private key if the key pair is generated before the Applicant's identity is verified and the private key is compromised.

2.1.4.2 SUBSCRIBER OBLIGATIONS

A Subscriber has the following obligations:

a. Not to divulge the value of any private key associated with its certificate to any other entity.

b. Provide password protection of the Subscriber's private key.

c. Notify the RA(s) or TRA(s) immediately if the Subscriber:
   1. No longer requires its private key;

   2. Has reason to believe that its private key has been compromised, or;

   3. No longer has access to its private key (Ex: Can not remember password that unlocks private key).

d. Destroy any private key that has been reported to the RA(s) or TRA(s) as compromised.

e. Use the certificate exclusively for authorized and legal purposes, consistent with this RPS, and follow the NOCA's procedures and instructions related to certificates.

f. Represent themselves accurately in all communications with the NOCA.

2.1.4.3 RELYING PARTY OBLIGATIONS

A Relying Party has the following obligations:

a. Use the Subscriber's certificate for the purposes indicated in the certificate information (e.g., the key usage extension).

b. Check each certificate for validity, using procedures described in the X.509 (2000), prior to reliance, and ensure that the reliance is reasonable in consideration of all facts listed in the certificate or incorporated in it by reference

c. Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment.

d. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.

e. Maintain contact with the Repository to keep informed of updates to policy, or this RPS, that may affect the reliance the Relying Party may choose to place on any certificate issued by the NOCA.

f. Use the certificate exclusively for authorized and legal purposes, consistent with this RPS, and follow the NOCA's procedures and instructions related to certificates.

g. Adhere to the rights and obligations covered by any cross certification agreement between the NOCA and any External Certificate Authority, if the Relying Party is a Subscriber of an External Certificate Authority.

2.1.4.4 PKI SPONSOR OBLIGATIONS

Any PKI Sponsor is obligated to:

a. Work with the RA(s) to register components (routers, firewalls, etc.);

b. Meeting the obligations of Subscribers as defined throughout this RPS.

2.1.5 Repository Obligations

Repositories that support the NOCA in posting information must:

a. Maintain availability of the information as required by the certificate information posting and retrieval stipulations of the NOCA CPS, and;

b. Provide access control mechanisms sufficient to protect repository information.

2.2 LIABILITY

2.2.1 CA Liability

The NOCA makes no warranties or representations, express or implied, concerning the production, use and maintenance of certificates under the NOCA CP, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided.

The NOCA supports, and will attempt to resolve, functionality problems that arise out of the use of cryptographic software distributed by the NOCA. Other commercial software not distributed by the NOCA is supported on a case-by-case basis. The end user is responsible for obtaining support for cryptographic software not supported by the NOCA, and must ensure they are operating in accordance to Federal Information Processing Standards (Ex: FIPS 140-2).

The NOCA accepts no liability for indirect, special, incidental or consequential damages, or for any loss of profits, loss of data, or other indirect consequential or punitive damages arising from or in connection with its services. The NOCA is not liable for any loss:

a. Of interruptions due to war, natural disasters, or other uncontrollable forces.

b. Incurred between the time that a certificate is revoked and the next scheduled issuance.

c. For actions arising from use of a certificate for which the Subscriber fails to comply with the NOCA CP and from use or reliance of any other policy referenced in the NOCA CP.

d. Caused by unauthorized, fraudulent or negligent use of certificates.

e. Due to the compromise of the Subscriber's private key and for loss due to inaccuracy of information provided by the Subscriber.

2.2.2 RA Liability

The RA is solely responsible for any claims of loss related to the non-performance of the RA's duties in accordance this RPS, all affiliated certificate policies, and other agreements.

2.2.3 Subscriber Liability

The Subscriber is solely responsible for meeting its obligations under this RPS. Failure of the Subscriber to comply with this RPS is grounds for certificate revocation. The Subscriber waives any and all claims against the Service, its agents and employees, contractors and assignees for any action arising from the use or possession of the certificate.

2.2.4 Relying Party Liability

Relying Parties, at their own discretion and risk, may use certificates in accordance with this RPS. The Relying Party is solely responsible for making the determination whether to use the certificate and for any resulting liability or loss. The Relying Party who fails to meet any of its obligations or to comply with this RPS waives any and all claims against the Service, its agents and employees, contractors and assignees for any action arising from the use or possession of the certificate.

2.3 FINANCIAL RESPONSIBILITY

This section is not applicable to the RPS.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The federal laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this RPS

2.4.2 Jurisdiction

Jurisdiction will be in the federal courts of the District of Columbia.

2.4.3 Severability, Survival, Merger, Notice

If any part of this RPS is unenforceable, the validity of the remaining parts will not be affected. This RPS constitutes the full understanding of the parties with respect to certificate practices; however, other terms and conditions may apply if they incorporate by reference this RPS.

2.4.4 Dispute Resolution Procedures

There is no formal dispute resolution procedure for a controversy, dispute or claim arising out of or relating to the RPS. However, the PMA and Treasury PMO will attempt to resolve any disputes associated with the use of the certificates issued by the NOCA. Each party is responsible for their own fees and costs associated with any dispute.

2.5 FEES

This section is not applicable to the RPS.

2.6 PUBLICATION & REPOSITORY

2.6.1 Publication of CA Information

The NOCA will use an on-line Repository that is available to Subscribers and Relying Parties, which contains:

a. Subscriber certificates;

b. Certificate status information (ex: CRLs);

c. The root CA certificate;

d. Subscriber documentation.

Public key certificates and certificate status information published in the Repository will be publicly available.

2.6.2 Frequency Of Publication

All information outlined in section 2.3.1 will be published promptly and in accordance with section 4.4.9 after such information is available to the NOCA.

2.6.3 Access Controls

The NOCA will protect any repository information it maintains that is not intended for public dissemination. Certificates and CRLs are available via the NASA PKI Directory and are read only. Only the NOCA has read/write and delete privileges.

2.6.4 Repositories

The repository for certificates, CRLs and ARLs issued by the NOCA is provided by the NASA PKI directory system. The directory service provides uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency Of Compliance Audit

The NOCA will be subject to an annual compliance audit. The NOCA reserves the right to require periodic compliance audits or inspections of RA operations. Further, the PMA reserves the right to inspect any information in the control or custody of any RA pertaining to their identity proofing duties, or other obligations outlined within the NOCA CP. A full and formal annual traceability audit on the NOCA is to be performed during the fourth quarter of each government fiscal year. The PMA has the right to request a periodic audit or inspection of administrative NOCA operations.

2.7.2 Identity/Qualifications of Auditor

The auditor must demonstrate competence in the field of compliance audits and Government Auditing Standards as well as be familiar with this RPS and any related documentation. The auditor will provide proof of existing customers that have used their services in an auditor capacity. Independent and reputable auditors, approved by the Treasury PMA and the Treasury PMO, will perform audits.

2.7.3 Auditor's Relationship to Audited Party

The compliance auditor will be the PMA, the Office of the Treasury Inspector General (OIG), or a private firm selected by the PMA. The private firm must be independent from the entity being audited, or it will be sufficiently separated from that entity to provide an unbiased & independent evaluation.

2.7.4 Topics Covered by Audit

This RPS, in its entirety, as well as all other documentation supporting the NOCA is subject to annual compliance audits.

2.7.5 Actions Taken as a Result of Deficiency

The compliance auditor will report the results of a compliance audit to the PMA. The PMA will report the results to NASA. The NASA and the RA being audited will propose a remedy, including the expected time for completion, to the PMA. Depending upon the nature and severity of the discrepancy, the PMA, in its sole discretion, may decide to halt temporarily the RA operation of the entity, to revoke a certificate issued to the entity, or take other actions it deems appropriate. Upon correction of the deficiency, the PMA may reinstate the entity. The PMA may require a special compliance audit to confirm the implementation and effectiveness of the remedy.

2.7.6 Communication of Results

The compliance auditor will report the results of a compliance audit to the PMA, the Treasury PKI PMO and the Treasury CIO. The implementation of remedies will be communicated to the Treasury PKI PMO from the PMA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY OF INFORMATION

2.8.1 Types Of Information To Be Kept Confidential

Information that is stored locally on the RA equipment and is Sensitive But Unclassified (SBU), will be handled and protected as defined in the NASA Procedural Requirement NPR 1600.1 and NPR 2810.1A. (Note: A definition of SBU is provided in Chapter 10 of the NPR 1600.1.) Access will be restricted to Trusted Administration with a reason to know the information in order to perform their official duties.

2.8.2 Types Of Information Not Considered Confidential

A certificate will only contain information that is relevant and necessary to affect secure transactions such as the Subject name, E-Mail address, and Organization name. The information that is embedded in the certificate, such as the Subject name, E-Mail address, and Organization name are not considered confidential.

For the purpose of proper administration of the certificates, non-certificate information may be requested to manage the certificates (Ex: identifying numbers, business addresses, telephone numbers, etc.).

2.8.3 Disclosure Of Certificate Revocation Information

Certificate status information is disclosed via the Repository to the general public.

2.8.4 Release to Law Enforcement Officials

The private decryption key that corresponds to a public key in an encryption certificate is escrowed and stored in the NOCA internal database, or it's electronic archive. In the event a subscriber is suspected to have used, or is using their digital credentials to commit illegal acts under the governing laws of the United States of America, upon presentation and verification of official court order or subpoena documentation and approval from Treasury General Counsel, this key pair will be disclosed to law enforcement officials to assist in any investigative process.

Any request for release of information will have its documentation authenticated. The authentication process requires that the receiver of the request:

- Verify the presenting official's credentials (at least one government-issued photo I.D.)
- Verify the subpoena or court order documentation presented by the official. This includes a sight check of the official letterhead and original signature, in addition to contacting the issuing office as specified on the document
- Notifying the Treasury PKI PMO prior to releasing the requested information

2.8.5 Release As Part Of Civil Discovery

Information will be released in connection with civil discovery by subpoena, court order or otherwise as required by law. Unless prohibited by the terms of the order under which the civil discovery is proceeding, the NOCA will make reasonable efforts to notify the end entity prior to releasing the information.

2.8.6 Disclosure Upon Subscriber's Request

The NOCA will release Subscriber information maintained by the NOCA pertaining to the certificate application, or actions leading to the issuance of the Subscriber's certificate, with the prior written consent of the Subscriber.

2.8.7 Other Information Release Circumstances

The NOCA will not disclose non-certificate information to any third party unless authorized by the NOCA CP, required by federal law or regulation, or order of a court of competent jurisdiction.

2.9 INTELLECTUAL PROPERTY RIGHTS

The U.S. Government retains exclusive rights to the intellectual property associated with any products or information developed under the NOCA CPS. Applicants and Subscribers represent and warrant that all information supplied during the certificate application process does not infringe upon or violate the intellectual property rights of any third party. Applicants and Subscribers will defend, indemnify, and absolve from financial responsibility the NOCA for any claims of loss or damage resulting from such infringement or violation. If Applicants and Subscribers find it impossible to comply with this provision because Federal or State law prohibits indemnification or other compensation, the NOCA will waive this provision because compliance would be contrary to law.

2.9.1 General

The intellectual property in this RPS is the exclusive property of NASA.

2.9.2 Certificates and OIDs

Copyrights and all other intellectual rights contained in the Certificates and registered OIDs are the property of the U.S. Government and may only be used in accordance with the NOCA CPS. Any other use of the above without the express written permission of the U.S. Government is expressly prohibited.

2.9.3 Private Keys

NOCA private keys are controlled via the procedures and processes incorporated from the implementation of a hardware security module (HSM), which is a FIPS 140 Level 3 approved device.

3. Identification & Authentication

3.1 INITIAL REGISTRATION

3.1.1 Types Of Names

The NOCA can issue certificates under various levels of assurance. Currently NASA uses the Medium (Software) level and Device certificates. NASA will be suing the Medium (Hardware) level when HSPD-12 Authentication Certificates are issued.

For certificates issued under Medium (Software), Medium (Hardware), and Device, the NOCA generates and signs certificates that contain an X.500 DN. For interoperation within the Federal Public Key Infrastructure (FPKI), NASA uses an X.501 distinguished name specifying a geo-political name.

All geo-political X.501 distinguished names assigned to NASA subscribers are in one of the following directory information trees:

C=US, o=U.S. Government, ou=NASA, ou=PIV
C=US, o=U.S. Government, ou=NASA, ou=People

The distinguished name of the subscriber will take the following form:

C=US, o=U.S. Government, ou=NASA, [ou=department], cn=nickname lastname+uid=AgencyUID

The nickname may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known.

X.501 distinguished names assigned to federal contractors and other affiliated persons will be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take the following form:

C=US, o=U.S. Government, ou=NASA, [ou=department], cn=nickname lastname (affiliate)+uid=AgencyUID

To ensure uniqueness across the agency, NASA will supplement the name forms for users by including a user id (uid) attribute as part of a multi-valued RDN with the common name.

Devices or non-people certificates that are the subject of certificates are assigned a geo-political name
Device names may take the following form:

C=US, o=U.S. Government, ou=NASA, ou=Services, cn=device name

where device name is a descriptive name for the device.

There is not intent for the NOCA to issue subordinate CA certificates, however, this addresses the NOCA distinguished name. The NOCA will use the following naming convention:

C=US, o=U.S. Government, ou=NASA, ou=Certification Authorities, ou=NASA Operational CA

The NOCA reserves the right to issue certificates using any of the above naming conventions in order to prevent duplication of Subscriber names.

For certificates issued under Authentication, assignment of X.500 distinguished names is optional. If assigned, distinguished names will follow the rules specified above for Medium (Hardware). Certificates issued under Authentication will include a subject alternative name. At a minimum, the subject alternative name extension will include the pivFASC-N name type. The value for this name will be the FASC-N of the subject's PIV card.

It should be noted that at the time of this RPS publication, NASA does not have a requirement for Card Authentication Certificates, therefore name types for these certificates are not included in this RPS.

3.1.2 Need For Names To Be Meaningful

The Issuer name that is placed in every certificate the NOCA issues will match the subject name in the NOCA certificate.

Subject names used in certificates identify the person or object in which they are assigned in a meaningful way. For X.500 based DNs, the common name represents the Subscriber in a way that is easily understandable for humans. For individuals, the legal name will be used. For equipment, this may be a model name and serial number, a server's fully qualified host name, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

3.1.3 Rules For Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in [USGold]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.4 Uniqueness Of Names

The NASA Office of the CIO will enforce name uniqueness across the NASA PKI. DNs are guaranteed to be unique throughout the NASA PKI and must never be reused.

The NOCA enforces name uniqueness within its X.500 name space. A Common Name (CN) in the NOCA's X.500 name space normally identifies the Subscriber. The CN consists of the Subscriber's Nickname and Last names. To ensure uniqueness, the X.500 DN will consist of a multi-valued Relative Distinguished Name (RDN) composed of the above-mentioned CN and a User ID. Refer to section 3.1.1 for specific examples.

3.1.5 Name Claim Dispute Resolution Procedure

The NASA Office of the CIO, will attempt to resolve any name collisions brought to its attention.

3.1.6 Recognition, Authentication And Roles Of Trademarks

The NOCA and PMA will not generally seek evidence of trademarks, court orders, or any other right to use the Subject Name prior to issuance. The NOCA will not generally issue or reissue a certificate with a particular Subject Name even if the certificate application contains a registered trademark owned by the Applicant or for which the Applicant has submitted a trademark registration application.

3.1.7 Method To Prove Possession Of Private Key

Since end entities generate their own signature keys, the NOCA requires proof of possession of the private key. This is done by the end entity using its private key to sign a value and providing that value to the NOCA, using the PKIX-CMP (RFC-2510). In some cases, SSL/TLS may be used as a proxy mechanism in combination with PKIX-CMP. This will occur via the use of the following products:

- Entrust Enrollment Server for the Web
- Entrust Security Manager Proxy

3.1.8 Authentication Of Organization Identity

Public-key certificates are issued to individuals whenever possible. For those cases where there are several individuals acting in one capacity, a certificate may be issued that contains the name of an organization.

An application for an organization must be made by an individual who will o act on behalf of the prospective Subscriber (i.e. organization). The requester must have already been issued a digital certificate by the NOCA [i.e. a current Subscriber]. This individual must be the person in the organization who will be responsible for ensuring control of the certificates and the associated private keys, including accounting for which individual of the organization has control of the keys at what time. In addition, in the case of an organization, the confidentiality (i.e. encryption) key pair shall be used but the digital signature key pair shall not be used.

Identification and authentication of the prospective Subscriber is as follows:

- Requests for organizational certificates include the organization name, address, and;
  - For organizations or groups within NASA, the prospective Subscriber shall possess a valid NASA identity and been issued a digital certificate by the NOCA, the Subscriber shall include their name and badge number on the request
  - For business organizations or partners outside of NASA, the prospective Subscriber shall provide the notarized copies of documentation providing the evidence of the existence of the organization [i.e. articles of incorporation]
- RA verifies the identity and authority of the individual acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization;
  - For organizations or groups within NASA:
    - RAs must verify valid identity of prospective Subscriber through a confirmation from the Center Protective Services or if the RA is resident in the Center

Protective Services through a check of the NASA Identity Management Systems (IDMS)

- For business organizations or partners outside of NASA:
  - RAs retain copies of the notarized copies of the documents providing evidence of the organizations existence
  - Where notarized documents are not feasible the RA shall authenticate:
    - the organization using existing business agreements between NASA and the organization, or
    - using searches of recognized databases of registered corporations

- RA keeps a record of the organization documents presented
  - If required to perform an authentication check, the RA keeps a record of the details of the check to include date, databases used and results of the check

- RA shall retain the name of the person to whom the organizational certificate is issued

The procedures for issuing organizational certificates do not conflict with other stipulations of this RPS (e.g., key generation, private key protection, and Subscriber obligations).

3.1.9 Authentication Of Individual Identity

RAs have always had the requirement to verify an individual's identity before issuing a certificate. The introduction of Homeland Security Presidential Directive #12 (HSPD-12) and the accompanying guidance provided in FIPS-201-1, has raised this requirement of identity verification as a pre-requisite for access to Federal facilities and IT systems.

In concert with other federal agencies, NASA has established identity proofing processes to meet the Federal Information Processing Standard (FIPS) 201-1, Personal Identity Verification (PIV-I) requirements. The PIV-I identity proofing requirements and the NOCA CPS requirements are similar. NASA will use its PIV-I processes to meet the NOCA CPS individual identity authentication requirements. NASA's identity proofing processes is provided in Appendix B. Appendix C provides a cross reference between the requirements for individual identity authentication stated in the NOCA CPS, and NASA's PIV-I processes.

3.1.9.1 Authentication Of Subscriber's Identity

3.1.9.1.1 NOCA CPS Requirements for Authentication of Subscriber's Identity

The NOCA CPS states that the minimum authentication procedures must include:

NASA Employees [Civil Servants]:

1.) Verify that a request for certificate issuance to the applicant was submitted by the agency management

2.) Applicant employment is verified through use of official agency records.

3.) Applicant identity established by in-person proofing before the RA. This in-person proofing can follow one of two processes. (See In-Person Proofing)

4.) A biometric of the applicant [fingerprint or photograph] will be recorded and maintained by the RA or CA.

Contractors or other affiliated personnel:

1.) Verify that a request for certificate issuance to the applicant was approved by an authorized sponsoring NASA employee, (e.g. Contracting Officer (CO) or Contracting Officer Technical Representative (COTR))

2.) Verify the Sponsoring NASA employee's identity and employment through:
   a. A digital signature verified by a currently valid employee signature certificate issued by the NOCA, may be accepted as proof of both employment and identity or
   b. By in-person proofing before the RA (See step 3) and employment validated through use of official agency records.

3.) Applicant's identity will be established by in-person proofing before the RA based on one of the two processes (See In-Person Proofing)

4.) A biometric of the applicant [fingerprint or photograph] will be recorded and maintained by the RA or CA.

Additionally:

RA will record the process that was followed for issuance of each certificate. The documentation will include:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).
  Reference the format set forth in 28 U.S.C. 1746
  Within the United States, its territories, possessions, or commonwealths:
  " I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date).
  (Signature)".
  Without the United States, its territories, possessions, or commonwealths:

"I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date).

(Signature)".

(See Appendix D for more information on 28 USC. 1746)

In-Person Proofing
The in-person proofing options noted below apply to NASA Civil Servants and Contractors or other affiliated personnel. The RA can perform in-person proofing based on either of the following processes:

Process #1:

1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

2. The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and

3. The credential presented in step 1) above will be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

Process #2:

1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

2. The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a photograph of applicant securely stored and linked to the credential), and

3. The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the identifying information (e.g., name and address) on the credential presented in step 1) above will be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.]

3.1.9.1.2 NASA RA Process for Authentication of Subscriber's Identity - In Person Proofing

The requirements stated in FIPS 20-1 and the NOCA CPS change the NASA RA processes. The identity proofing processes in FIPS 201-1 and the NOCA CPS require that the NASA RA function include the NASA Center's Protective Services. NASA Center's Protective Services organizations have the personnel who are authorized to perform background investigations and identity proofing. Additionally the NASA Center's Protective Services have the equipment to

capture biometrics and have the resources to check and retain as needed identity documents. For all these reasons, the NASA Center's Protective Services will perform the authentication of a subscriber's identity.

As noted earlier, NASA will use its PIV-I processes to meet the NOCA CPS requirements for Subscriber identity authentication. For on-site NASA employees and contractors or affiliates identity proofing should be done before or at the time of Entry-on-Duty, therefore the status of the background investigation will be available for determining if the applicant can be issued a certificate.

NASA is following PIV-I processes and using Federal Agencies to verify Subscriber identity, therefore for most Subscribers, NASA will not use Process #1 or #2. For more information on the NASA identity verification process, please consult Appendix B. If a Subscriber's identity cannot be verified through the PIV-1 process, then RAs will use Process #1.

3.1.9.1.3 NASA RA Process for Authentication of Subscriber Identity - Off Site

Where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The requirements for off site subscriber identity authentication are:

- the trusted agent forwards the information collected from the applicant directly to the RA in a secure manner
- recording a biometric of the applicant may be satisfied by providing passport-style photographs to a notary.
- the trusted agent will verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package
    - packages secured in a tamper-evident manner by the trusted agent satisfy this requirement.

RAs are still responsible for performing steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), above.

3.1.10 Authentication Of Devices Or Applications

If an Applicant is a system component (e.g., a server), the Applicant will be represented by a human sponsor already issued a digital certificate by the NOCA [i.e. a current Subscriber]. Application must be made by an individual to whom the device or application is attributable.

The Subscriber will present information sufficient for registration at the level of the certificate being requested, The Subscriber must maintain operational control of, and responsibility for, certificates issued to the device or process along with the associated private keys.

This Subscriber provides the following registration information:

a) Date of the application request

b) Requester (Subscriber) Name [First, Last]

c) Requester (Subscriber) Center Name

d) Requester (Subscriber) Contact Information [email address and telephone number

e) If the Requester is not the owner of the device/application then they are to provide;
    1. Owner Name [First, Last]
    2. Owner Email Address

f) Device DNS Name

g) Purpose - the intended use of the device, web server, application. To include the NASA project name associated with the device, server, application;

The Requester will digitally sign the request thus verifying their association with NASA. If the Requester is not the Owner, an email will be sent to the Owner notifying them that a certificate request for a device/application/server was made under the name of the Requester and if the request is not correct to contact the RA.

3.2 AUTHENTICATION FOR CERTIFICATE RENEWAL, UPDATE AND ROUTINE REKEY

Re-keying a certificate means that that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key; a different serial number; and may be assigned a different validity period.

NASA civil servants and on-site contractors key certificates are updated automatically.
As such, both the encryption and digital signature key pairs are automatically updated prior to expiration. Prior to expiration of the current key pairs, the NOCA software invokes the operation of a secure communications protocol and the Subscriber's keys are updated transparently.

The exception to this is the Subscriber's Authentication certificate which will be assigned an expiration date and will not be automatically updated. Upon or before expiration, NASA Subscribers will follow the FIPS 201-1 guidelines for re-issuance of an Authentication certificate.

3.2.1 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. Subscriber certificates issued by the NOCA will not be renewed.

FIPS 201-1 outlines criteria for card renewal. Card renewal will be managed through the ActivIdentity Card Management System. In the case of card renewal a new Authentication key/certificate will be issued but the Subscriber does not repeat full registration. NASA is in the process of understanding the ActivIdentity Card Management System and developing a process for requesting card renewal.

3.2.2 Certificate Re-Key

Re-keying a certificate means that a new certificate is created that has the same characteristics and the assurance level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and is assigned a different validity period.

A certificate will be re-keyed only if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

The public key lifetimes given are maximums. A program may always require shorter lifetimes. Signature private keys should be stopped from usage some time before the public key expires. The key management private key can be used any time to decrypt the information. The following public key lifetimes are for Subscribers and RAs; CA key lifetimes are provided in Section 4.7:

Assurance Level	Public Key Certificate Life Times
Medium (Software) Medium (Hardware) Authentication Device Card Authentication	Signature and key management keys re-key every three years.

For the various assurance levels, upon re-key, the subscribers will be authenticated as listed below:

Assurance Level	Routine Re-Key Identification and Authentication Requirements for Subscriber Certificates
Medium (Software) Medium (Hardware) Authentication Device Card Authentication	Identity may be established through use of current signature key, except that identity will be established through initial registration process at least once every six years from the time of initial registration and in the case of PIV Card re-issuance. Per FIPS 201-1, Section 5.3.2.2, "In case of re-issuance, the entire registration and issuance process including fingerprint and facial image capture shall be conducted."

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued. If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.

Finally, when the NOCA updates its private signature key and thus generates a new public key, the CA will notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. This notification will primarily occur by way of publishing a new CA certificate to the Repository. NOCA will generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users.

3.3 AUTHENTICATION FOR REKEY AFTER REVOCATION

For Subscribers whose certificates [Authentication, Key Management, Digital Signature] have been revoked, rekey is not permitted until the initial registration process [outlined in section 3.1] is repeated, except in the following situations:

For Key Management or Digital Signature certificates only:

- an organizational change within NASA results in changes to the Distinguished Names of several employees

- a Subscriber is temporarily unable to present himself or herself in person (e.g. on extended travel) and the revocation was not due to a key compromise in which case re-key must meet the criteria for certificate issuance to geographically remote Subscribers.

3.4 AUTHENTICATION OF REVOCATION REQUEST

Revocation requests must be authenticated. See Section 4.4.2.

4. Operational Requirements

This section describes the processes used in the certificate lifecycle management. For information on use of the RA software please refer to the product documentation or the NASA PKI Registration Authority Operations.

4.1 Application For A Certificate

For NASA personnel both civil servants and contractors to whom a PIV Card is issued, the certificate request application is subsumed under this PIV Card request process. No additional application needs to be made.

Personnel who are not issued a PIV card will have to submit an application for certificate. The certificate request application includes:

- the Requester's full name
- the Requester's citizenship
- the Requester's type of NASA affiliation (civil servant/contractor/partner)
- if a contractor or partner
  - full name of the requester's NASA Sponsor
  - Sponsor's NASA Center
  - Sponsor's email and telephone number
- the Requester's work e-mail address
- the Requester's work telephone number
- acknowledgement of the terms specified in the Subscriber Agreement using the wording below:
  - I acknowledge and declare that, prior to applying for, accepting or using the NASA Public Key Certificate, I have read and accepted the conditions in the NASA PKI Subscriber Agreement. The NASA PKI Subscriber Agreement is available on the Internet at http://nasaca.nasa.gov/docs.html. I accept the subscriber obligations and responsibilities contained therein as described in the NASA PKI Subscriber Agreement.

    I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief.
- date and signature of Requester
- date and signature of Sponsor [for contractors/partners]

The Requester signs and dates the request.

A Sponsor co-signs and dates for contractors or partners. For partners, the sponsoring civil servant signs and dates the request. For contractors, the Sponsor can be a civil servant Sponsor or the requesting contractor's COTR or Technical Monitor.

The Subscriber acknowledgement of his or her obligations [defined in section 2.1.4.2] is included in the certificate request application. The Requester's signature on the application serves as the handwritten signature evidence for Subscriber acknowledgement.
The RA will work with their Center Protective Services to confirm Sponsor's identity and association with NASA by verifying a PIV Card has been issued to the Sponsor. Sponsor and Requester will be contacted to initiate background investigation for requester, per Section 3.1. The Center Protective Services staff confirms that an investigation is initiated or complete by sending a secure message to the RA. Based on the verification, the RA either accepts or refuses the certificate request. The RA notifies the Requester of acceptance or refusal. The RA notes the action taken on the certificate request, the date of the confirmation/denial from Protective Services and then signs and dates the request. The RA retains the certificate request.

4.2 CERTIFICATE ISSUANCE

Upon receiving the confirmation that identity investigation is initiated or in progress from the Center Protective Services, the RAs:

- Depending on the Subscriber's cryptographic software or module, complete the issuance using one of the processes below if all certificate requirements has been met.

For issuance of the Authentication Certificate [PIV Authentication certificate, the RA use the ActivIdentity Operator interface to issue the Authentication certificate to the PV Card. Steps for issuance through the ActivIdentity interface are described in the NASA PKI PIV Card Operator Manual.

For issuance of Key Management and Digital Signature certificates, the RA uses the Entrust RA interface. The RA:

1. To initiate issuance, the Subscriber must have an entry in the NASA PKI Directory. If the Subscribers entry cannot be found, the RA contacts the PKI Technical Support to resolve the issue.

2. The RA logs in to the CA server through the RA interface software to create a certificate for the Subscriber. The RA enables the Subscriber using the Subscriber's Distinguished Name from the NASA PKI Directory and records the event in the RA Administrator Logbook. The enabling operation results in the creation of authorization information that the RA securely distributes to the Subscriber. The Subscriber needs the authorization information to initially log in and complete the key and certificate generation process.

3. The RA contacts the Subscriber for collection of the Subscriber's authorization information. Subscribers present themselves in person to receive their authorization information. To receive the authorization information, the Subscriber presents picture identification to the RA to provide confirmation that he/she is indeed the person who requested the certificate. With this confirmation, the RA provides the Subscriber with the

authorization information. The Subscriber is informed to use the authorization information within 5 working days of receipt of the authorization information and agree not to divulge this information prior to their initialization.

4. To complete the certificate issuance process, the PKI client software is installed on the Subscriber's computer. The Subscriber logs in to the PKI client and enters the authorization information provided to him/her. A secure communication is established between the Subscriber's PKI client software and the NOCA. Delivery of key pairs is described in section 4.2.1 and 4.2.2.

If the RA must issue certificates to Subscribers who are not in the same geographical location as the RA, the RA and the Subscriber arrange a process in which the authorization information can be securely delivered to the Subscriber and the Subscriber can confirm their identity remotely.

The issuance and publication of a certificate by the NOCA indicates a complete and final approval of the certificate application.

4.2.1 Delivery of Public Key for Certificate Issuance

All communications between the NOCA and the Subscriber will be authenticated and protected from modification. This will be done using mechanisms commensurate with or stronger than the requirements of the data to be protected.

Public keys must be delivered for certificate issuance in a way that binds the applicant principal's verified identification to the public key.

For Key Management keys, the NOCA generates the Subscriber's Key Management key pair. Therefore, there is no required delivery mechanism to the NOCA for the Key Management public key.

In some cases, SSL/TLS may be used as a proxy mechanism in combination with PKIX-CMP. This will occur via the use of the following products:

- Entrust Enrollment Server for the Web
- Entrust Security Manager Proxy

If the SSL/TLS protocol is used as part of this process, the SSL/TLS server certificate key size must adhere to the key size requirements specified in section 6.1.5.

4.2.2 Delivery of Subscriber's Private Key to Subscriber

A Subscriber's digital signature private key will be generated by the Subscriber and will remain within the cryptographic boundary of the cryptographic module. Anyone who generates a private signing key for a Subscriber will not retain any copy of the key. Multiple Subscribers in the NASA PKI will not share private signing keys. Under no circumstances will anyone other than the Subscriber have knowledge of or control over private signing keys.

The Subscriber Key Management private key will be generated by the NOCA and delivered to the Subscriber via PKIX-CMP (RFC-2510).

4.2.3 CA Public Key Delivery to Subscribers

The public key of the Treasury Root CA, the Common Policy Root CA, and the subordinate NOCA, will be available for certification trust paths to be created and verified. The public key of the Treasury Root CA and Common Policy Root CA will appear in the form of a self-signed public key certificates.

The Treasury Root self-signed certificate, and the NOCA certificate, will be delivered to the Subscribers via PKIX-CMP (RFC-2510).

If the NOCA has, or will have, the ability to deliver the Common Policy Root CA certificate via PKIX-CMP (RFC-2510), it will do so. Otherwise, the Common Policy Root CA certificate will be delivered to the Subscribers via alternative methods. Acceptable methods for the self-signed certificate delivery include:

1. The NOCA loading the certificate onto tokens delivered to Subscribers via secure mechanisms;

2. Secure distribution of the certificates through secure out-of-band mechanisms;
    a. Ex: Subscriber, or Sponsor, receives a copy of the certificate on a floppy disk, or other media, from a RA, or TRA.

3. Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

4.3 CERTIFICATE ACCEPTANCE

The Subscriber is deemed to have accepted the certificate at the time the NOCA issues the certificate. The publication of a certificate in an active state by the NOCA constitutes a complete and final acceptance of the certificate by the Subscriber.

Acceptance by the Subscriber of his/her responsibilities regarding certificate use is secured in the certificate request process as described in section 4.1 of this RPS.

4.4 CERTIFICATE SUSPENSION & REVOCATION

4.4.1 Circumstances For Revocation

A certificate is revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- the Subscriber violates, or the NOCA suspects that the Subscriber is violating, the terms of this RPS, or any other agreement, regulation or law applicable to the certificate;

- the Subscriber is no longer affiliated with NASA;
    - ex: Subscriber's employment is terminated or Subscriber is suspended for cause

- compromise or suspected compromise of private keys and/or password and profile

- private key has been, or is suspected of having been lost, or stolen;
    - ex: computer on which profile is stored is lost or stolen

- change in Subscriber's role (such as organizational change between Centers) or permissions

- media holding the private key is compromised or suspected of compromise

- the Subscriber or other authorized party (as defined in section 4.4.2 requests that the certificate be revoked

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- the Subscriber in whose name the certificate has been issued

- the individual or organization who made the application for the certificate on behalf of a device or application

- the Subscriber's management, if the Subscriber is a NASA employee or contractor

- a TRA or an RA associated with the NOCA

- a NASA Center's Information Technology (IT) Security Manager

- NOCA personnel

- the Treasury PMA
    - The NOCA and PMA may request the revocation of any Subscriber's certificate(s). In the event this occurs, a written notice and brief explanation for the revocation is provided to the Subscriber via electronic or paper form.

4.4.3 Procedure For Revocation Request

Any individual identified in section 4.4.2 can initiate a revocation request. The requester must notify their local RA, complete and sign a request for revocation.

Revocation request forms must be obtained for auditing purposes and must contain the following information:

- date of revocation request

- name of the owner of the certificate (i.e. Subscriber)
- certificate owner's NASA organization (if applicable)
- detailed reason for requesting revocation
- name and title of person requesting revocation
- contact information of person requesting revocation
- signature of person requesting revocation

Revocation requests are sent to the RA. In cases requiring immediate revocation of a Subscriber's certificate an encrypted and signed email request or call must be sent to the RA.

The RA confirms the request:

- If the request is in paper form, the RA verifies the handwritten signature on the request form belongs to the person requesting revocation.
    - Ex:
        - Witnessing the requestor sign the form "in-person", or
        - Have the requester send the request as an attachment in digitally signed email message.

- If the request is in digital form, the RA validates the digital signature on the form, or embedded in the request data depending on the format of the request.
    - Ex:
        - A digital signature in an Adobe .PDF document or Filenet form.

Upon receipt and confirmation of the request, the RA revokes the Subscriber's certificate by logging in to the CA server and performing the certificate revocation. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the request and then signs and dates the request. The RA retains the revocation request.

When the RA performs a certificate revocation, the NOCA will revoke the associated certificate and place it on the CRL. Revoked certificates will be included on all new publications of the certificate status information indefinitely.

Revocation of a certificate of a person in a RA role will follow the procedures for completing and signing a request for revocation as noted in this section. The RA not being revoked, will send a signed and encrypted email to the NOCA SuperRA requesting that the role of the RA requesting revocation be changed from RA to User. The NOCA SuperRA will return a signed and encrypted email confirming the role change. The NOCA SuperRA records the event in the CA Officer Logbook. The RA not requesting revocation can then complete the action by performing the certificate revocation. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the written request and then signs and dates the request.

4.4.3.1 REVOKE AN AUTHENTICATION CERTIFICATE

NASA is in the process of understanding the ActivIdentity Card Management System interface. It is possible to revoke the Authentication certificate on the PIV Card through the ActivIdentity Card Management System interface. The processes described in sections 4.4.1, 4.4.2 and 4.4.3 will be used to request revocation of the Authentication certificate. The RA will follow the procedures noted in section 4.4.3 but execute the revocation action through the ActivIdentity Card Management System interface.

4.4.4 Revocation Request Grace Period

There is no grace period for certificate revocation. The NOCA will take immediate action to revoke a certificate upon receipt of a revocation action from an RA.

Key compromise, suspected key compromise, and dismissal for cause are identified as security incidents and are handled by locally defined IT security incident/response procedures at each NASA Center. Revocation requests for other revocation reasons must be submitted to an RA as soon as possible and no later than within 24 hours of the incident.

4.4.5 Circumstances For Suspension

The NOCA may disable/suspend a Subscriber's certificate if a Subscriber goes on leave. The NOCA may disable/suspend a Subscriber's certificate in support of a security investigation by internal NASA security personnel or external law enforcement agencies. Unlike revocation, disabling a Subscriber allows for re-enabling at a later time.

Information on public keys of disabled Subscribers is not available in the NASA PKI Directory, but it is retained in the NOCA database. Once the certificate is disabled/suspended, the Subscriber's keys are not available for authentication, encryption or signing. However, recipients may verify any files that were signed prior to the suspension.

4.4.6 Who Can Request Suspension

The parties identified in section 4.4.2 can also request disabling/suspending a certificate.

4.4.7 Procedure For Suspension Request

Any individual identified in section 4.4.2 can initiate a suspension request. The requester must notify their local RA, complete and sign a request for suspension.

Suspension requests are required for disable/suspension for auditing purposes and must contain the following information:

- date of suspension request
- name of the owner of the certificate (i.e. Subscriber)

- time period of suspension
- certificate owner's NASA organization (if applicable)
- detailed reason for requesting suspension
- name and title of person requesting suspension
- contact information of person requesting suspension
- signature of person requesting suspension

Suspension requests are sent to the RA. In cases requiring immediate suspension of a Subscriber's certificate either an encrypted and signed email or a call may be placed to the RA.

The RA confirms the request:

- If the request is in paper form, the RA verifies the handwritten signature on the request form belongs to the person requesting revocation.
    - Ex:
        - Witnessing the requestor sign the form "in-person", or
        - Have the requester send the request as an attachment in digitally signed email message.

- If the request is in digital form, the RA validates the digital signature on the form, or embedded in the request data depending on the format of the request.
    - Ex:
        - A digital signature in an Adobe .PDF document or Filenet form.

Upon receipt and confirmation of the suspension request, the RA disables the Subscriber by logging in to the CA server and performing the disable. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the suspension request and then signs and dates the request. The RA retains the suspension request.

Suspension of a certificate of a person in a RA role will follow the procedures for completing and signing a request for suspension as noted in this section. The RA not being suspended will send a signed and encrypted email to the SuperRA requesting that the role of the RA requesting suspension be changed from RA to User. The SuperRA will return a signed and encrypted email confirming the role change. The SuperRA records the event in the CA Officer logbook. The RA not being suspended can then complete the action by performing the certificate suspension. The RA records the event in the RA Administration Logbook. The RA notes the action taken on the suspension request and then signs and dates the request.

4.4.7.1 SUSPEND AN AUTHENTICATION CERTIFICATE

NASA is in the process of understanding the ActivIdentity Card Management System interface. It is possible to suspend a PIV card and the Authentication certificate on the PIV Card through the ActivIdentity Card Management System interface. The processes described in sections 4.4.5, 4.4.6 and 4.4.7 will be used to request suspension of the PIV Card and Authentication

certificate. The RA will follow the procedures noted in section 4.4.7 but execute the revocation action through the ActivIdentity Card Management System interface.

4.4.8 Limits On Suspension Period

The requesting party stipulates the suspension period in the suspension request.

4.4.9 CRL Issuance Frequency

The NOCA issues CRLs every 18 hours on a 24 X 7 basis even if no changes have been made. In the event of private key compromise or loss, the NOCA will immediately publish an updated CRL to the NOCA's Repository.

The NOCA is configured to not remove certificate serial numbers from the CRL upon expiry of the certificate.

4.4.10 CRL Checking Requirements

Relying Parties will determine how often new revocation data should be obtained.

Whenever feasible, before using a certificate, Relying Parties must check its status against a current copy of the CRL. The Relying Parties within NASA are provided PKI software that provides CRL information and verifies the NOCA's signature on the CRLs and ARLs. If it is temporarily infeasible to obtain revocation information, then the Relying Party must make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be verified or reject the use of the certificate.

4.4.11 On-line Revocation/status Checking Availability

The NOCA is currently researching an implementation of OCSP [RFC 2560], however, it does not offer OCSP services at the time of the publication of this RPS.

4.4.12 On-line Revocation Checking Requirements

Not applicable, per statement in 4.4.11

4.4.13 Other Forms Of Revocation Advertisements Available

PIV Authentication certificates are provided with information on alternate methods of revocation information.

4.4.14 Checking Requirements For Other Forms Of Revocation Advertisements

No requirements for checking, the http site is made available as an alternate form of revocation publication for PIV Authentication certificates.

4.4.15 Special Requirements Related To Key Compromise

In the event of private key compromise or loss, the NOCA will immediately publish a CRL and/or ARL.

4.5 SYSTEM SECURITY AUDIT PROCEDURES

Section 4.5 and subsequent subsections describe security auditing capabilities of the NOCA's operating system and CA applications and are not applicable to this RPS. For more information on this topic, please reference the "X.509 Certificate Policy for the US Treasury PKI".

This RPS does provide information on the Logbooks used by NASA RAs and CA Officers.

4.5.1 RA And CA Officer Logbooks

The purpose of the RA Administration Logbook and the CA Officer Logbook are to log events so that in cases in which the CA database must be recovered, the RA logbooks and CA Officer Logbook can be used to reconstruct events not captured on the last CA database backup.

The logbooks should be hardcover with numbered pages and stitched binding. Log entries should be entered in ink. Log entries should include the date and time an action was taken, a description of the action taken, the name of the person(s) executing the action, and the signature(s) or handwritten initials of the person(s).

The logbooks should be under the control of the respective RA and CA Officer personnel. When not in use it should be stored in a location accessible to the respective personnel. As the logbooks will be used for data recovery, the retention period of a logbook should be at least 3 months.

4.6 RECORDS ARCHIVAL

Section 4.6 and its subsequent subsections describe requirements for record archival. The sections in this RPS will address the archival requirements for RAs.

4.6.1 Types Of Data Retained

This section describes all the archival requirements as stated in the CPS. In the table below the RA archival items are noted in BOLD type.

At a minimum, the following data will be recorded for archive in accordance with each assurance:

Data To Be Archived	Medium (Software) Medium (Hardware) Authentication Device Card Authentication
CA accreditation (if applicable)	X
Certification Practice Statement	X
Contractual obligations	X
System and equipment configuration	X
Modifications and updates to system or configuration	X
Certificate requests	**X**
Revocation requests	**X**
Subscriber identity Authentication data as per Section 3.1.9	**X**
Documentation of receipt and acceptance of certificates	**X**
Documentation of receipt of tokens	**X**
All certificates issued or published	X
Record of CA Re-key	X
The last issued CRL at time of archival	X
All Audit Logs	X
Other data or applications to verify archive contents	X
Documentation required by compliance auditors	X
All Audit Summaries	X

4.6.1.1 TYPES OF DATA RETAINED

In the execution of the RA function, various documents are provided to the RAs:

- certificate requests/approvals for personnel not issued PIV Cards
- certificate suspension requests/approvals
- certificate revocation requests/approvals
- key recovery requests/ approvals

Protective Services organization at each NASA retain the following:

- identity Authentication data
- requests for PIV Card [include certificate request]
- receipts of PIV Card [i.e. token]

4.6.2 Retention Period for Archive

The archives are retained for a minimum period of 10 years and 6 months from the date of their creation.

If the original media cannot retain the data for the required period, the archived data will be transferred to other media pending the technologies available during the time of transfer.

4.6.3 Protection Of Archive

The documents retained by the RAs are stored is secure storage container to which only the RAs have access. The information retained by Protective Services is retained in secure storage in a facility with controlled access.

For more information on protection of CA archives, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

4.6.4 Archive Backup Procedures

Not applicable to the RPS.

For more information on backup of CA archives, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

4.6.5 Requirements for Time-Stamping of Records

Not applicable to the RPS.

For more information on time-stamping requirements for the CA, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

4.6.6 Archive Collection System

Not applicable to the RPS.

For more information on the collection system for CA archives, please reference the “X.509 Certificate Policy for the US Treasury PKI”

4.6.7 Procedures To Obtain And Verify Archive Information

Not applicable to the RPS.

For more information on procedures for obtaining and verifying CA archive information, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

4.7 KEY CHANGEOVER

4.7.1 CA Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired.

The key changeover procedure for the NOCA itself will be treated in the same manner as the initial key generation ceremony. A formal script will be used, and all activities related to the changeover process will be audited and witnessed by the Treasury PMA.

The NOCA’s signature key will be re-keyed every three (3) years, with a certificate validity period not to exceed six (6) years.

4.7.2 Subscriber Key Changeover

The process described in this section is automatic key update/changeover. For NASA Subscribers, their PIV Authentication certificate and key will not automatically update/changeover. Most NASA Subscribers [civil servants and on-site contractors] will have automatic key update for their Key Management [encryption] certificate/key and Signing certificate/key.

In automatic key update, the original and new private signing keys of the Subscriber will sign the request for a new signing certificate. Subscribers with automatic key update, the software

performs this action without the Subscribers direct knowledge. Subscribers' keys are given specific lifetimes. The private signing key lifetime is seventy percent (70%) of the lifetime of the certificate. This provides a transition period for the Subscriber, which is thirty percent (30%) of the lifetime of the certificate. If the Subscriber is unable to re-key within the transition period, the NOCA must set the user to recovery mode. The NOCA does not automatically re-key a Subscriber whose keys have already expired. A Subscriber whose keys have already expired must re-apply for a new certificate.

For Subscribers without automatic key update, must re-apply for new certificates/keys when their keys expire.

4.8 COMPROMISE AND DISASTER RECOVERY

Section 4.8 and subsequent subsections describe disaster recovery procedures for the CA and while not applicable to the RPS, some sections are included to provide information to the NASA RAs. For more information on this topic, please reference the "X.509 Certificate Policy for the US Treasury PKI".

It should be noted that this RPS includes a section on Entity Key Recovery, which is a RA procedure and process. Entity Key Recovery is described under section 4.8.1.

4.8.1 Computing Resources, Software, and/or Data Are Corrupted

This section in the RPS describes the procedures when a Subscriber's or RAs software profile is corrupted or they have forgotten their passwords for access to their software. To re-establish access the Subscriber's keys must be recovered.

It is important to note that the recovery process, applies to the Subscriber's key management and signing key pairs. Authentication keys/certificates will not be recovered. If for some reason an authentication key/certificate is damaged or corrupted, a new Authentication key/certificate will be issued. While certificates and keys are not recovered it is possible for a PIV Card user to forget their PIN. Procedures for PIN reset are described in section 4.8.1.5

For the Subscriber's key management and signing keys, the key recovery process disables a Subscriber's current key pairs and allows for the revision of profile data by any person in possession of the newly generated authorization information. Re-initialization then allows access to a Subscriber's previously encrypted files.

Key recovery is performed by local RAs. Two RAs are present to authorize and perform key recovery operations. If two RAs are unavailable, CA Officers or SuperRAs act as substitute administrators in emergency cases.

The timeframe for completion of non-emergency key recovery requests is within 48 hours. In emergency cases, the local RA is contacted.

4.8.1.1 KEY RECOVERY REQUESTED BY THE SUBSCRIBER

Examples of reasons for Subscriber requested key recovery include:

- a Subscriber forgets a password
  [see section 4.8.1.5 for PIN reset when user forgets PIN}

- a Subscriber loses or damages a PKI profile file

- a Subscriber loses or damages a security token (PCMCIA card) and encryption and signing keys are stored on the token

- a Subscriber suspects his/her keys have been compromised

4.8.1.1.1 KEY RECOVERY

For the Subscriber's protection from unauthorized requests, the Subscriber must a) submit a request to the RA stating the reason for the recovery and b) make arrangements to appear in person

Upon receipt of the request, the RAs visually verify the identity of the Subscriber using the employee badge, and perform the key recovery process. RAs log the recovery event for auditing purposes. The RAs note the action taken on the request, and then sign and date the request. The RAs retains the recovery request.

RAs then present the Subscriber with new authorization information.

If a Subscriber is temporarily unable to present himself or herself in person (e.g. on extended travel) and the recovery is due to forgotten password or a damaged profile file, recovery must meet the criteria for certificate issuance to geographically remote Subscribers.

4.8.1.2 KEY RECOVERY WITHOUT SUBSCRIBER CONSENT

Examples of reasons for key recovery without Subscriber consent include:

- a Subscriber has left the organization and the Subscriber's supervisor or department management needs to decrypt files for business continuity

- a Subscriber's actions are in question by the Center's IT Security Manager and the Subscriber's files need to be reviewed

- a Subscriber's actions are in question by an external law enforcement agency and the Subscriber's files need to be reviewed.

Key recovery without subscriber consent is always performed with RA intervention. In cases in which Subscribers are not aware of a key recovery operation, Subscribers shall not be able to log into the NASA CA system with their previous password. This will alert them that their accessibility has changed. Requesters have the responsibility to assess the impact of disclosure and upon doing so, may choose not to perform a key recovery.

When Subscribers discover that they can no longer access the their keys, they most likely will contact the RA for assistance. Based on instructions from the requester, the RA disseminates information to Subscribers accordingly.

The key recovery requester needs to contact their local Center IT Security Manager. Written approval from both the Subscriber's management and from the Center IT Security Manager requesting key recovery action is submitted to the RAs before the action is performed. The request must contain the following:

- date of recovery request
- name of the owner of the keys (i.e. Subscriber)
- keys owner's NASA organization (if applicable)
- requester's name and NASA organization
- detailed reason for requesting access to Subscriber's files
- specific name(s) of person(s) allowed to see Subscriber's files and to be responsible for subsequent viewing by any unnamed persons
- description (and/or filename(s)) of Subscriber's files to be viewed, *or* statement of approval to access all files
- description of RA's role beyond key recovery action, including what information to provide if the Subscriber should inquire about the change in their NOCA accessibility
- NASA Center IT Security Manager and the employee's management position titles signatures, and dates of signatures.

Request forms are sent to the RAs. Upon receipt, the RAs contact the appropriate parties to schedule key recovery actions.

Note: In certain situations, RAs may be given a court order requesting key recovery. In this case, the court order will be the equivalent of a written approval.

If applicable, requesters should bring a removable or portable memory storage device containing Subscriber's files to be viewed at the scheduled recovery process. RAs may load files on a local machine for decrypting/viewing and then delete decrypted files at the completion of the process, avoiding potential unauthorized viewing.

Requesters should first confirm that the RAs have machines with the required software to view the files. If not, the RAs may travel to the requester's location within the NASA site.

Upon receipt of request, the RAs visually verify the identity of authorized person(s) using the employee badge, perform the key recovery process, and log the recovery event. The RAs note the action taken on the request, and then sign and date the request form. The RAs retain the request for auditing purposes.

If the Subscriber will be retaining accessibility privileges to the NOCA after the requested key recovery is completed, the RAs perform another key recovery process so the Subscriber may be ensured that no one has access to their key data any longer.

When applicable, the RAs may disable the recovered Subscriber's NOCA account after the scheduled process if a short, remote viewing time limit has been requested. Re-enabling the account shall be based on instructions provided by the requester.

4.8.1.3 KEY RECOVERY FOR RA

CA Officers or SuperRAs perform key recoveries for RAs. Two CA Officers or SuperRAs are present to authorize and perform key recovery operations.

The timeframe for completion of non-emergency key recovery requests is within 48 hours. Centers should indicate in their correspondence with the NOCA Technical Support if an emergency recovery is required.

The NASA Technical Support will maintain, "shared secrets" for each RA. These secrets will not be sensitive in nature (such as driver's license, social security number, etc.) but should be something known only to the individual. This database will be maintained in a secure manner. This database will be used to verify the identity of the RA prior to recovery.

When a RA needs to be recovered, the following steps will be followed:

The RA request for recovery will be sent to the NOCA Technical Support.

The RA will complete a request for recovery and fax it to the NOCA Technical Support or in the case of an electronic form, email the form to the NOCA Technical Support.

When the form is received the NOCA CA Officer or SuperRA will contact the RA and prompt the RA for two of the supplied shared secrets chosen randomly from the database.

After receiving the correct responses from the RA, the NOCA CA Officers or SuperRAs recover the RA, records the action in the CA Officer logbook. The CA Officer or SuperRA notes the action taken on the form, signs and dates the form, and retains the recovery form.

4.8.1.4 KEY RECOVERY REQUESTED BY EXTERNAL ENTITY

External entities refer to any law enforcement agency (FBI, DEA, State Police, etc). Requests by an external entity must be processed through the NASA Center's IT Security Manager.

The steps in section 4.8.1.2 are followed for external entity requests.

4.8.1.5 PIN RESET

The PIN on a PIV Card may need to be reset if the contents of the card are locked resulting from the usage of an invalid PIN more than the allowed number of retries stipulated by the NASA. [i.e. user forgets their PIN]

The criteria for PIN reset per FIPS 201-1:

- before the reset PIV Card is provided back to the cardholder, the card issuer shall

ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card

NASA is in the process of understanding the ActivIdentity Card Management System interface. At this time NASA has not defined a process for PIN reset. This RPS will be updated when the PIN reset process is defined.

4.8.2 Public Key is Revoked

If the NOCAs public keys are revoked for any reason, the following will occur:

1. The appropriate authoritative party will coordinate with the Treasury PMO to revoke the NOCAs certificate and publish the appropriate ARL/CRL.

2. The NOCA system will be regenerated with a new set of NOCA keys. The initial key generation script will be followed, and all activities pursuant to the changeover process will be audited and videotaped.

4.8.3 CA Private Key Compromise

In the event of a CA private key compromise, the following operations must be performed:

- Immediately notify the Federal PKI Policy Authority and the Treasury PMA

- Generate a new signing key pair and corresponding Trusted Certificate

- Initiate procedures to notify subscribers of the compromise; and

- All current subscribers will repeat the initial registration process outlined in section 3.1.

All Relying Parties or Subscribers not registered in the Repository or certificate management software are responsible for periodically checking the Repository for such notification.

4.8.4 CA Private Key Loss

If the NOCA 's equipment is damaged or rendered inoperative, and the NOCA 's signature keys are destroyed, the NOCA will take the following actions:

1. The Common Policy PA and Treasury PMA will be notified.

2. All Subscribers, Relying Parties, and other end users registered in the Repository and certificate management software will be notified of the loss;

3. A notification of the loss will be published in the Repository;

4. At the discretion of the PMA, a new CA key pair will be generated, and all Subscribers who were registered and active prior to the CA private key's destruction will be re-enrolled under the new CA.
    - A new NOCA will be established using build and Key Generation Ceremony scripts

- Directory Administrators will restore the repository (if needed)
- A [CA] Security Officer will find all valid certificates within the repository
- The [CA] Security Officer will create a bulk operations script to add all of the previous valid users to the new CA
- The RA will deliver the resulting Reference Numbers and Authorization Codes to the Subscriber.

All Relying Parties or other Subscribers not registered in the Repository or certificate management software are responsible for periodically checking the Repository for such notification.

4.8.5 Secure Facility After a Natural or Other Type of Disaster

The PMO will make several operational determinations in the event of a natural or other type of disaster:

1. The PMO will determine whether the NOCA private signing key has been compromised. This determination will be based on whether the disaster has created a less secure operating environment for the NOCA than what is specified in the CPS. If the NOCA private signing key is compromised, the procedure for revocation will be followed.

2. The PMO will determine whether the NOCA has been rendered inoperative by the disaster. If inoperative, the PMA will designate the Contingency & Alternate Processing Site (CAPS) facility as the primary NOCA site.

The results of these decisions will be communicated, either through email, pager, telephone, or in person, by the PMO to at least two NOCA personnel. Immediately following this communication, the following procedures will be followed:

A [CA] Security Officer (SO) will send a digitally signed message, using their NOCA-issued credentials, to the appropriate parties of the current situation. Status messages will be sent daily until the NOCA is operational.

4.8.6 CA Cannot Generate CRLs

If the NOCA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the Common Policy PA and Treasury PMA will be informed.

4.9 CA TERMINATION

In the event of termination of the NOCA's operation, the CAs, and RAs will coordinate to revoke all certificates issued by the NOCA. The NOCA will send formal written notification to all organizations it has issued certificates to, notifying them of its termination. In addition, the NOCA will notify each organization representative informally via email, pager, voicemail, or telephone. The PMA will inform all cross-certified CAs, so that cross-certificates to the NOCA may be revoked. Prior to CA termination, the PMA will direct the NOCA to provide archived

data either to the PMA or other approved archival facility. Archived data will also be retained as described in section 4.6 or as directed by the PMA.

5. Physical, Procedural & Personnel Security

5.1 PHYSICAL CONTROLS

Section 5.1 and subsequent subsections describe physical controls of the NOCA and are not applicable to this RPS. For more information on this topic, please reference the "X.509 Certificate Policy for the US Treasury PKI".

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

This section and subsequent subsections describe the trusted roles that comprise the NASA PKI. NASA personnel or US Treasury personnel fulfill these trusted roles. Trusted roles that are performed by Treasury personnel include:

- NOCA CA Administrator
- Operator
- Auditor

Trusted roles that are performed by NASA personnel include:

- Directory Administrator
- [CA] Security Officer
- RA

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy.

5.2.1.1 NOCA CA ADMINISTRATOR

The NOCA Administrator role is responsible for the operation and maintenance of the NOCA server. This includes:

a. Software Back-ups:
   - Operating system
   - Operating system logs
   - Incremental back-ups (Once per day)

- Full back-ups (Once per seven days)

b. Monitors the NOCA software application platform and reports services down;

c. Performs operation and maintenance of the NOCA hardware and operating system;

d. Executes script/routines that manage operating system log creation and deletion on the NOCA;

e. Initiates Change Control procedures for Operating System upgrades and/or patches, and

Administrators do not issue certificates to Subscribers.

5.2.1.2 NOCA OPERATOR

The NOCA Operator provides day-to-day administration of tape backups associated with the NOCA system(s), which include performing backups of the NOCA server's operating system(s) and logs.

5.2.1.3 DIRECTORY ADMINISTRATOR

The Directory Administrator role is responsible for the operation and maintenance of the NASA PKI Directory server. This includes:

a. Perform back-ups

b. Coordinate/install software updates and patches

c. Confirm and update current anti-virus and other security software updates

d. When necessary, restart server(s)

5.2.1.4 [CA] SECURITY OFFICER

The [CA] Security Officer role is responsible for:

a. setting and modifying the security policy for the NOCA, in accordance with the CPS and the X.509 Certificate Policy;

b. setting the number of required authorizations for sensitive operations;
c. adding and deleting other CA Officers, and RAs;

d. changing CA Officer and RA password rules;

e. setting default certificate lifetimes;

f. if necessary, acting as a Substitute RA

5.2.1.5 RA

The RA/ role is responsible for:

a. accept and process certificate issuance, certificate change, certificate revocation/suspension and key recovery requests

b. verify of an applicant's identity

c. transmit applicant information to the CA

d. receive and distribute Subscriber authorization information

The procedure manual for this role is the NASA PKI Registration Authority (RA) Operations Manual.

5.2.1.6 NOCA AUDITOR

The auditor role is responsible for:

a. Reviewing, maintaining, and archiving audit logs, and;

b. Performing or overseeing internal compliance audits to ensure that the NOCA is operating in accordance with its CPS.

5.2.2 Separation of Roles

Individuals may assume more than one role, however, the roles of Administrator, Officer, Auditor, and Operator may not be shared. For example, an Administrator cannot also have an Officer, Auditor, or Operator role, and so on. The NOCA system will identify and authenticate its users and will ensure that no user identity can assume more than one of the Administrator, Officer, Auditor, and Operator roles.

5.2.3 Number of Persons Required Per Task

Sensitive functions are separated to preclude any one individual from gaining the opportunity to adversely affect the computer system. Separation of duties or M of N authentication is required for sensitive administrative operations such as CA key backup.

The following tasks are defined as sensitive and require at least two individuals to perform the tasks. These individuals use a split knowledge technique of two password entries and verification to perform any sensitive operation.

Two [CA] Security Officers are required to:

- add and delete other CA Officers and RAs; and

- set default certificate lifetimes;

- cross certify with other CAs.

Two RAs are required to:

- perform in person key recovery

5.2.4 Identification and Authentication for Each Role

Identification and authentication mechanisms, such as passwords and tokens, are used to control account access for each role. All access by each role to accounts requires password and/or token identification and authentication.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

As it pertains to Treasury personnel involved in NOCA operations:

- All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens.

- Treasury management is responsible for screening all Treasury NOCA Employees, an Agent, or their contractors to ensure a level of trust comparable with the duties of the individual.
    - This complies with the Office of Personnel Management (OPM) human resource guidelines for a standard security background check.

- Treasury management is responsible for ensuring that appropriate background investigations are conducted on Treasury NOCA and contractor personnel assigned to sensitive positions.

- Procedures for Treasury NOCA personnel have also been established to immediately revoke access privileges to individuals being separated for cause.
    - A number of technical, operational, and management controls are used to prevent and detect harm.
    - Such controls include individual accountability, least privilege, and separation of duties.

RA personnel will be appointed by approving authorities at NASA Centers. Each NASA Center has a PKI Point-of-Contact (POC). The PKI POC will notify NASA PKI Operations of potential new RAs. The PKI POC will provide NASA PKI Operations a copy of the RAs clearance or a memo signed by the Center's Protective Services personnel confirming the clearance for the RA. The RA will study this RPS, the RA Manual and practice using the PKI Administrative software. The RA will sign a statement, confirming that he/she has read the required documents and practiced using the software. When the RA is ready, the RA will be interviewed on his/her understanding of the NASA PKI policies/procedures. If the RA obtains a 70% or

higher result on their interview and all other required paperwork has been received by NASA PKI Operations, the RA will be approved.

The NASA roles of [CA] Security Officer and RA roles are deemed to be positions of "Public Trust" per the Office of Personnel Management (OPM) 5 CFR Parts 731, 732, and 736. Personnel filling these roles shall successfully complete investigations for Public Trust positions.

As regards TRAs, the NASA POCs will work with parties that wish to establish a TRA relationship with their respective RAs.. The requesting organization must identify the TRA(s) for their organization in writing to the PKI POC. To the greatest extent possible TRA personnel should be personnel who are trusted within the requesting organization. The requesting organization provides the proposed TRAs full legal name, email address, and other contact information using a signed hard copy request. This request will be sent to the NASA PKI POC and the NASA PKI POC will send a copy of this request to the NASA PKI Operations.

5.3.2 Background Check Procedures

Treasury personnel operating the NOCAs will have a Single Scope Background Investigation using the Standard Form 86, "*Questionnaire for National Security Positions*".

For NASA personnel, all background checks are performed in accordance with NASA Personnel Security Policies.

5.3.3 Training Requirements

As pertains to Treasury personnel involved in NOCA operation:

- All trusted personnel attend focused training before performing their duties.

- In addition to technical training, trusted personnel receive training with regard to data handling to ensure confidential information, records and applications are handled in compliance with the Privacy Act, if applicable.

- After the initial training, new personnel are trained by existing operators of the equipment. In addition, periodic training on the technologies used to support the infrastructure operations of the NOCA is available. Such courses may include, but are not limited to:
    - Entrust Authority Security Manager Comprehensive
    - Entrust Authority Security Toolkit for Java Developers
    - End User Basic Computer Security Awareness
    - Building More Secure Information Systems (FISMA)
    - Solaris System Performance Management
    - Solaris System Administration for Experienced UNIX Administrators
    - Certification & Accreditation: C&A Process for IT Security Reviews

New NASA RAs are required to:

- training in the operation of the software using a test NOCA environment

- review the RA Operations Manual, and the RPS

5.3.4 Retraining Frequency And Requirements

As pertains to Treasury personnel involved in NOCA operation:

- All Trusted Administration of the NOCA will receive new training when a major system upgrade is implemented or new operating procedures are introduced. NOCA Administrators will receive re-training or additional training, as needed.

The RA training environment and manuals noted in section 5.3.3 are kept current to accommodate changes in the NOCA system. Refresher training is conducted in accordance with these changes.

5.3.5 Sanctions for Unauthorized Actions

All personnel who have access to data on any NOCA computers/networks are responsible for the data and are bound by applicable laws, rules, and NOCA directives.

NASA RA personnel that operate in violation of the policies and procedures stated herein may have their access to the NOCA system revoked and may be subject to administrative discipline and possible criminal prosecution.

Repeated or significant violations of this RPS may result in revocation of the NASA PKI Operations or RA personnel public key certificates.

5.3.6 Contracting Personnel Requirements

As pertains to Treasury personnel involved in NOCA operations

- All contracting personnel must follow guidelines comparable to section 5.3.1 (Background and Qualifications).

- In the event that contractor personnel wishes to make use of subcontractors, final approval over the use of the subcontractor will required from the Treasury PMA.

- All contractor personnel whom provide any services to the NOCA will establish procedures to ensure that any subcontractors perform in accordance with the Common Policy, the Treasury Certificate Policy and the CPS.

As pertains to NASA personnel involved in NOCA and NASA PKI operation:

- Contractor personnel employed to operate any part of the NASA CA or RAs are subject to the same criteria as a US Government employee, and cleared to the level specified in section 5.3.1.

5.3.7 Documentation Supplied to Personnel

As pertains to Treasury personnel involved in NOCA operations

- Trusted Administration who operate the NOCA are provided with written operational procedures, which are reviewed and updated by the NOCA and/or PMA.
    - The individual duties and responsibilities of personnel are further documented in the employee's position description. The duties and responsibilities of contractor employees are stipulated in the terms and conditions of the contract.
- NOCA will make available to its CA, RA personnel the certificate policies it supports, and relevant parts of the CP, and any relevant statutes, policies or contracts.

As pertains to NASA personnel:

- This RPS is made available to the NASA CA and RA personnel and to Subscribers.

- Operation manuals are made available to CA Officer and RA personnel so they can operate the PKI software.

- In addition to this RPS, the Subscribers are provided information on the use and protection of the software used within the NASA domain.

5.3.7.1 PROCEDURES RESIDING IN OTHER DOCUMENTATION

A structure as complex as the NOCA will rarely be described or driven by a single document. There are several other documents available for normal operating procedures.

Additional procedural documentation is included in various product administration manuals, and training guides from Entrust Technologies.

6. Technical Security Controls

Section 6 and subsequent subsections describe technical security controls of the NOCA and are not applicable to this RPS. Information on certain sub-sections is provided in this RPS to provide information to the NASA RAs.

Certain cryptographic software or modules used by the Subscriber affect how keys and corresponding certificates are generated and further managed. Specific operations performed by particular cryptographic software packages or modules should be included within any associated vendors' documentation.

6.1 KEY PAIR GENERATION AND INSTALLATION

Section 6.1 and subsequent subsections describe key generation and installation of the NOCA and are not applicable to this RPS. This section is provided in the RPS to provide information to the NASA RAs.

6.1.1 Key Pair Generation

Requirements for generation of pseudo-random numbers, key pairs and symmetric keys for the NOCA, RA, and Subscribers are listed in Section 6.2.1.

In circumstances where the Subscriber's cryptographic software or module manages two separate key pairs, the NOCA creates all of the Subscriber's encryption key pairs and corresponding encryption certificates.

Any software key generation process performed by cryptographic software and associated modules must comply, at a minimum, with the requirements of FIPS 140 Level 2.

CA key pair generation will occur under the direction of a Key Generation Ceremony script. The key generation ceremony is one of the most sensitive operations in the CA system's lifecycle, which the script incorporates the detailed procedures for separation of duties and M of N initialization and activation. This script identifies all of the explicit procedures, command sequences, and separation of roles during the evolution of the key generation event. Throughout the event, the CA system software will electronically log each event process as it relates to the operation of the CA software. Further, any corrective measures taken during the event must be reported within an addendum to the script, or within an official witness or auditor report.

6.1.2 Private Key Delivery To Entity

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When the NOCA generates keys on behalf of the Subscriber, the private key is delivered securely to the Subscriber. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber will not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key is protected from activation, compromise, or modification during the delivery process.
- The Subscriber will acknowledge receipt of the private key(s) via PKIX-CMP (RFC-2510).
- The key material is encrypted using PKIX-CMP (RFC-2510). The Subscriber, upon receipt of the private keys, generates the activation data.

In circumstances where the Subscriber's cryptographic software or module manages two separate key pairs, the NOCA delivers the Subscriber's encryption private key to the Subscriber via the PKIX-CMP (RFC-2510).

6.1.3 Public Key Delivery To Certificate Issuer

Where the Subscriber, or RA generates key pairs, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism will bind the Subscriber's verified identity to the public key. The NOCA makes use of PKIX-CMP (RFC-2510) to achieve this binding.

In circumstances where the Subscriber's cryptographic software or module manages two separate key pairs, the NOCA generates the Subscriber's encryption key pair. Therefore, there is no required delivery mechanism to the NOCA.

In some cases, TLS may be used as a proxy mechanism in combination with PKIX-CMP. This will occur via the use of the following products:

- Entrust Enrollment Server for the Web
- Entrust Security Manager Proxy

6.1.4 CA Public Key Delivery To Users

The NOCA delivers its public key certificate to the Subscriber via PKIX-CMP (RFC-2510) during the registration process.

When a CA updates its signature key pair, a key rollover certificate published to the directory will distinguish the new CA key. Key rollover certificates are signed with the CA's current private key, so secure distribution is not performed.

In cases where the CA certificate is not delivered to the Subscriber, the Subscriber is responsible for obtaining the CA certificate using the mechanism defined in section 4.2.2.

6.1.5 Asymmetric Key Sizes

Certificates issued by the NOCA will contain no less than 1024 bit RSA keys and SHA-1 in accordance with FIPS 186-2. Certificates that expire on or after December 31, 2010 will contain at least 2048 bit RSA keys and SHA-256.

End entity certificates issued under Authentication, Card Authentication, Device that expire before December 31, 2010 will contain RSA public keys that are at least 1024 bits in length. End entity certificates issued under Authentication, Card Authentication, and Device that expire on or after December 31, 2010 will contain RSA public keys that are at least 2048 bits.

End entity certificates issued under Medium (Software) and Medium (Hardware) that expire before December 31, 2008 will contain RSA public keys that are at least 1024 bits in length. End entity certificates issued under Medium (Software) and Medium (Hardware) that expire on or after December 31, 2008 will contain RSA public keys that are at least 2048 bits.

Use of TLS or another protocol providing security for the NOCA operations will use at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA through 12/31/08. After 12/31/08, AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA keys will be used. The following are a list of cipher suites that are required where SSL/TLS is used:

Cipher Suite	Authentication	Key Establishment	Encryption	Digest
NIST SP-800-52 Recommended				
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DSS	DHE	AES_256_CBC	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	RSA	DHE	AES_256_CBC	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DSS	DH	AES_256_CBC	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	RSA	DH	AES_256_CBC	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DSS	DHE	AES_128_CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	RSA	DHE	AES_128_CBC	SHA-1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	SHA-1
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DSS	DH	AES_128_CBC	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	RSA	DH	AES_128_CBC	SHA-1
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DSS	DHE	3DES_EDE_CBC	SHA-1
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DHE	3DES_EDE_CBC	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	SHA-1
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	DSS	DH	3DES_EDE_CBC	SHA-1
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	RSA	DH	3DES_EDE_CBC	SHA-1
OpenSSL 1.0 - FIPS				
DHE-RSA-AES256-SHA	RSA	DHE	AES_256_CBC	SHA-1
DHE-DSS-AES256-SHA	DSS	DHE	AES_256_CBC	SHA-1
AES256-SHA	RSA	RSA	AES_256_CBC	SHA-1

Cipher Suite	Authentication	Key Establishment	Encryption	Digest
EDH-RSA-DES-CBC3-SHA	RSA	DH	3DES_EDE_CBC	SHA-1
EDH-DSS-DES-CBC3-SHA	DSS	DH	3DES_EDE_CBC	SHA-1
DES-CBC3-SHA	RSA	RSA	3DES_EDE_CBC	SHA-1
DHE-RSA-AES128-SHA	RSA	DHE	AES_128_CBC	SHA-1
DHE-DSS-AES128-SHA	DSS	DHE	AES_128_CBC	SHA-1
AES128-SHA	RSA	RSA	AES_128_CBC	SHA-1
Entrust Security Manager Proxy				
RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	SHA-1

CRLs issued by the NOCA will use the SHA-1 hash algorithm when generating digital signatures. RSA signatures on CRLs that expire on or after December 31, 2010 will be generated using SHA-256.

Under some circumstances, the CA software is not capable of restricting key sizes (i.e. when keys are generated by clients). In these cases, the NOCA monitors the directory daily for any certificates issued with keys sizes less than 1024 bits. If such a key is discovered, then the NOCA will send notification to a RA to revoke the certificate, as described in section 4.4.4, and issues a new one with the proper key size.

6.1.6 Public Key Parameters Generation

At this time, the NOCA uses the algorithm sha1WithRSAEncryption. Depending on the parameter (i.e., encoding, algorithm identifier, etc) refer to PKCS-1 for documentation regarding the use of the algorithm. Entrust Technologies claims compliance with the following standards, where additional parameters may be used:

- RSA in accordance with Public Key Cryptographic Standards (PKCS) specification PKCS#1 Version 2.0, ANSI X9.31, IEEE 1363, ISO/IEC 14888-3 and U.S. FIPS PUB 186-2 (1024-bit, 2048-bit, 4096-bit and 6144-bit supported)

- RSA key transfer in accordance with RFC 1421 and RFC 1423 (PEM), PKCS#1 Version 2.0, IEEE P1363

- Diffie-Hellman key agreement in accordance with PKCS#3

- Simple Public-Key GSS-API Mechanism (SPKM) authentication and key agreement in accordance with RFC 2025, ISO/IEC 9798-3 and U.S. FIPS PUB 196

Otherwise, this section is not applicable.

6.1.7 Parameter Quality Checking

Refer to section 6.1.6.

6.1.8 Hardware/software Key Generation

Key generation will be performed as described in section 6.1.1.

6.1.9 Key Usage Purposes (as per X.509v3 key usage field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into subscriber user certificates will be used only for signing or encrypting, but not both. User certificates that assert id-fpki-common-authentication or id-fpki-common-cardAuth will only assert the *digitalSignature* bit. Other user certificates to be used for digital signatures will assert the *digitalSignature* and *nonRepudiation* bits. User certificates that contain RSA public keys that are to be used for key transport will assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement will assert the *keyAgreement* bit.

Public keys that are bound into CA certificates will be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates will assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs will assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses will assert the *digitalSignature* and *nonRepudiation* bits.

Public keys that are bound into device certificates may be used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) will assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport will assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement will assert the *keyAgreement* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits will not be asserted in certificates issued under this policy.

6.2 PRIVATE KEY PROTECTION

Section 6.2 and subsequent subsections describe the technical and procedural techniques for private key protection and sections applicable to this RPS are sections describing Subscriber private key protection. This section is included in the RPS to provide information to the NASA RAs.

It should be noted, however, that the protections noted below do not negate the Subscriber's responsibility to protect their private keys from disclosure. Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). Subscriber's private keys are secured through cryptographic mechanisms. In the case, where a Subscriber chooses to export their keys using PKCS#12, the stipulations for private key protection noted previously apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

6.2.1 Standards For Cryptographic- module

All cryptographic modules that provide for the storage, generation, and processing of keys will be FIPS-140 validated.

The table below summarizes the minimum requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA FIPS 140 Level	RA FIPS 140 Level	Subscriber FIPS 140 Level
Medium (Software)	3 (Hardware)	2 (Hardware)	2 (Software)
Medium (Hardware) Authentication Device Card Authentication	3 (Hardware)	2 (Hardware)	2 (Hardware)

6.2.2 Private Key (m of n) Multi-person Control

The NOCA makes use of SafeNet Luna CA3 cryptographic devices. These devices are configured for multi-token activation.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. All key pairs that are stored in the NOCA's certificate management software's database are encrypted. Retrieval of the escrowed keys occurs via PKIX-CMP (RFC-2510).

Under no circumstances will a subscriber signature key be held in trust by a third party.

6.2.4 Private Key Backup

If applicable, the Subscriber's encryption key pair is backed up in the NOCA 's encrypted certificate management software’s database.

6.2.4.1 NOCA PRIVATE SIGNATURE KEY BACKUP

A NOCA private signature keys will be backed-up under the same multi-person control as the original signature key. At most, two backup copies of the NOCA private signature key will be created and stored at PMA approved contingency facilities.

6.2.4.2 SUBSCRIBER PRIVATE SIGNATURE KEY BACKUP

Subscriber private signature keys will not be backed-up, escrowed, or copied

6.2.4.3 SUBSCRIBER PRIVATE DECRYPTION KEY BACKUP

Subscriber private decryption keys may be backed up however, they must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.5 Private Key Archival

Private signature keys will not be archived.

The history of all decryption private keys used by a Subscriber is maintained in the NOCA 's encrypted certificate management software's database.

6.2.6 Private Key Entry Into Cryptographic Module

Subscriber keys will be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

The NOCA keys are generated during the NOCA Key Generation Ceremony, which occur by and in the NOCA hardware cryptographic module's partition.

6.2.7 Method Of Activating Private Key

For certificates issued under Card Authentication, subscriber authentication is not required to use the associated private key.

For all other certificates, the subscriber must be authenticated to the cryptographic token before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data will be protected from disclosure (i.e., the data should not be displayed while it is entered).

For the CA, the cryptographic module must be activated for communication with the NOCA's certificate management software.

6.2.8 Method Of Deactivating Private Key

The private keys remain active for the period of login. The login period is ended either by:

a. Manually logging out of cryptographic module;

b. Destroying the process which keeps the module active;

c. Automatically, as determined by a preset timer;

d. Removing the hardware token (if applicable).

Subscribers with hardware tokens will be required to remove the hardware token as part of the logout procedure.

In the case, where a Subscriber chooses to export their keys using PKCS#12, the stipulations for private key deactivation for the ending of the login period, apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

For the CA, the cryptographic module must be deactivated for communication with the NOCA's certificate management software when not in use.

6.2.9 Method Of Destroying Private Key

Private signature keys will be destroyed in accordance with FIPS 140 when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

In the case, where a Subscriber chooses to export their keys using PKCS#12, the stipulations for destroying private key noted previously in the paragraph above apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

For the CA, the cryptographic module must be destroyed when no longer needed after the archival requirement, or upon replacing the hardware.

6.3 Other Aspects of Key Pair Management

A Subscriber's key-pair that is used for digital signatures will never be escrowed, archived or backed up, because a Subscriber can repudiate a transaction if there is a copy of his or her digital signature private key in existence.

For information that is encrypted, the Subscriber will use his or her private encryption (confidentiality) key to decrypt the information. If that private key is lost or destroyed, or if the Subscriber departs the agency without relinquishing the private key, or acts maliciously, there is no way to decrypt the information. Thus, for business continuity reasons, NOCA will escrow private keys used for decrypting data.

6.3.1 Public Key Archival

Public encryption keys are stored in the Repository. The NOCA also periodically backs up all keys except for Subscriber private signing keys.

6.3.2 Usage Periods For The Public And Private Keys

The usage period for the NOCA key pair is a maximum of six years. All Certificates and CRLs signed by a specific CA key pair will expire before the end of that key pair's usage period. The CA private key is used to sign Certificates and CRLs for up to a maximum of 3 years.

Subscriber public keys have a maximum usage period of 3 years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

The requirements for the NOCA keys are described in Section 4.7, Key Changeover.

The requirements for RA and Subscriber keys are described in Section 3.2, Certificate Renewal.

6.4 ACTIVATION DATA

Section 6.4 and subsequent subsections describe the technical and procedural techniques for activation data. These and sections are applicable to this RPS as they include activation data used by Subscribers and RAs. This section is provided in the RPS to provide information to the NASA RAs.

6.4.1 Activation Data Generation And Installation

The activation data used to unlock private keys, in conjunction with any other access control, will have an appropriate level of strength for the keys or data to be protected. The Subscriber or Sponsor will generate activation data in conformance with FIPS 112. This includes activation data for the PIV Card. The PIN policy established in the ActivIdentity Card Management System will conform to FIPS 112 as applicable and criteria defined in FIPS 201-1, Section 4.1.6.1.

In the case, where a Subscriber chooses to export their keys using PKCS#12, the password [activation data] generation requirements noted in the paragraph above apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

The Reference Number and Authorization Code generated for new subscribers, for retrieving certificates, could also be considered "activation data". Refer to section 4.1 for additional information.

6.4.2 Other Aspects Of Activation Data

Activation data in this section refers to activation data associated with the PIV Card [i.e. PIN} and activation data associated with soft cryptographic implementation [i.e. Entrust profile and keys] Activation data used to unlock private keys will be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

Activation data will be memorized, not written down. If written down, it will be secured at the level of the data that the associated cryptographic module is used to protect, and will not be stored with the cryptographic module. The protection mechanism will include a facility to temporarily lock the account after a predetermined number of login attempts as set forth in the CP.

In the case, where a Subscriber chooses to export their keys using PKCS#12, the password [activation data] protection stipulations of original passwords never stored, application termination or lockout after a predetermined number of login attempts and passwords never shared apply to all exportations of the private key and the storage mechanisms/locations of the exported private key.

6.5 COMPUTER SECURITY CONTROLS

Section 6.5 describes computer security controls for the NOCA and is not applicable to this RPS. For more information on this topic, please reference the "X.509 Certificate Policy for the US Treasury PKI".

6.6 LIFE CYCLE TECHNICAL CONTROLS

Section 6.6 and subsequent subsections describe life cycle technical controls, which mostly apply to the NOCA, some items apply to the RA. This section is provided in the RPS to provide information to the NASA RAs.
Updates to the system are performed using evaluated software and hardware and are implemented using a formal configuration management methodology.

Lifecycle technical controls:

- Hardware and software procured to operate a NOCA, or RA will be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

- Hardware and software developed for the NOCA, or RA will be developed in a controlled environment, and the development process will be defined and documented.

- All hardware and software will be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the final physical location.

- The NOCA hardware and software is dedicated to performing the CA functionality. There are no other applications, hardware devices, network connections, or component software, which are not part of the CA operation.

- Proper care will be taken to prevent malicious software from being loaded onto the NOCA /RA/ equipment. Only applications required to perform the operation of the CA will be obtained from sources authorized by local policy. RA hardware and software will be scanned for malicious code on first use and periodically afterward.

- Hardware and software updates will be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

Lifecycle technical controls as pertains to the RA:

- RA software can be run on a common PC platform therefore NASA Centers use existing procurement vehicles to procure RA hardware.

- RA systems use the Entrust software so no special software or hardware is developed or required.

- RA systems are dedicated to performing the RA function.

- RA systems are routinely scanned and patched as part of the NASA Center IT Security procedures and policies.

- RA software updates are performed through System Administrators who have completed certification.

6.6.1 Certificate Definition Change Procedures

6.6.1.1 BACKGROUND

It may become necessary to extend certificate definitions to include new business requirements. The process for change must be tightly controlled, allowing for flexibility, but maintaining the integrity, reputation, and security of the NOCA.

6.6.1.2 PROCEDURES

The steps to extend a certificate definition are as follows:

1. A certificate change request is submitted to the PMA outlining the change and its justification.

2. The PMA chairs consider the request and sign approved requests.

3. Upon notification of an approved request, the SO implements the change.

4. The SO and NOCA Auditor review the change before the change is implemented in the NOCA.

6.7 SECURITY MANAGEMENT CONTROLS

Section 6.7 describes security management controls for the NOCA and is not applicable to this RPS. For more information on this topic, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

6.8 NETWORK SECURITY CONTROLS

Section 6.7 describes network security controls for the NOCA and is not applicable to this RPS. For more information on this topic, please reference the “X.509 Certificate Policy for the US Treasury PKI”.

6.9 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Refer to section 6.2 “*Private Key Protection*"

7. Certificate & CRL Profiles

Section 7 and subsequent subsections describe the specifications of the certificates and CRLs issued by the NOCA and are not applicable to this RPS. This section is included in the RPS to provide information to the NASA RAs.

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

The NOCA will issue X.509 v3 certificates.

7.1.2 Certificate Extensions

Certificate extensions used by the NOCA will conform to the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF].

7.1.3 Algorithm Object Identifiers

Certificates will be issued with one of the following OIDs to identify the signature algorithms used by the holder of the certificate:

Signature Algorithm	OID
sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued by the NOCA will use the SHA-256 hash algorithm when generating RSA-PSS signatures. The following OID will be used to specify the hash in an RSA-PSS digital signature:

Subject Key Algorithm	OID
SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840)

Subject Key Algorithm	OID
	organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates will be issued with one of the following OIDs to identify the algorithm with which the subject key was generated:

Subject Key Algorithm	OID
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters will be specified as one of the following named curves:

Named Curve	OID
ansip192r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1}
ansit163k1	{iso(1) identified-organization(3) certicom(132) curve(0) 1}
ansit163r2	{iso(1) identified-organization(3) certicom(132) curve(0) 15}
ansip224r1	{iso(1) identified-organization(3) certicom(132) curve(0) 33}
ansit233k1	{iso(1) identified-organization(3) certicom(132) curve(0) 26}
ansit233r1	{iso(1) identified-organization(3) certicom(132) curve(0) 27}
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansit283k1	{iso(1) identified-organization(3) certicom(132) curve(0) 16}

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base certificate will be populated with an X.500 Distinguished Name as specified in section 3.1.1.

If the certificate issued under Authentication or Card Authentication, the subject alternative name extension shall be present and include the pivFASC-N name type as defined in section 3.1.1.

7.1.5 Name Constraints

The NOCA will not use the name constraints extension.

7.1.6 Certificate Policy Object Identifier

Certificates issued by the NOCA will assert the OID appropriate to the level of assurance with which it was issued, per Section 1.2.

7.1.7 Processing Semantics For The Critical Certificate Policy

Certificates issued by the NOCA will not contain a critical certificate policy extension.

7.1.8 Policy Qualifiers Syntax And Semantics

Certificates issued by the NOCA will not contain policy qualifiers.

7.1.9 Key Usage Constraints for id-fpki-common-authentication

Certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth must include a critical keyUsage extension, asserting only digitalSignature value.

7.2 CRL PROFILE

CRLs issued by the NOCA conform to the CRL Profile specified in [CCP-PROF].

7.2.1 Version Number(s)

CRLs issued by the NOCA are X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

A number of X.509 version 2 CRL and CRL entry extensions are used. These are outlined in the following table:

X.509 v2 CRL Extension	Critical/Non Critical	Optional	Notes
AuthorityKeyIdentifier	Non critical	Not optional	Only element [0] (authorityKeyIdentifier) is filled in contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	Non critical	Not optional	Incremented each time a particular CRL/ARL is signed
ReasonCode	Non critical	Not optional	CRL entry extension - only reason codes (0), (1), (3), (4) and (5) supported
IssuingDistributionPoint	Critical	Not optional	This extension is not included in combined CRLs

X.509 v2 CRL Extension	Critical/Non Critical	Optional	Notes
			element [0] (distributionPoint) includes the full DN of the distribution point element [1] (onlyContainsUserCerts) is included for CRLs element [2] (onlyContainsCACerts) is included for ARLs element [1] and [2] are never present together in the same revocation list elements [3] and [4] are not used

7.3 CERTIFICATE TYPE DEFINITIONS

The following certificate definitions are an initial listing, which may be expanded upon. For example, "Device - Web Server" & "Medium (Hardware) - Signature" could be combined to form a new definition (i.e., "Device - WS - Hardware"). The formation of such a definition will be approved in a formal change request to the PMA.

7.3.1 Enterprise Certificates

The Enterprise certificate type is an Entrust Profile containing Two (2) certificates. One certificate is used for authentication and digital signatures, and the other is used for encryption.

7.3.1.1 MEDIUM (HARDWARE)

This is an Enterprise certificate type that is stored in hardware, and asserts the “Medium (Hardware)” OID values.

7.3.1.2 MEDIUM (SOFTWARE)

This is an Enterprise certificate type that is stored in software, and asserts the “Medium (Software)” OID values.

7.3.1.3 DEVICE - PROFILE SERVER

This certificate type is used with the Entrust Roaming Server. This Entrust Profile is used to encrypt and decrypt Entrust profiles as they are stored, and retrieved, from the directory as well as to the remote client.

7.3.2 Web Certificates

A Web Certificate type is a single certificate that may be used to represent a person or a device. Automated key management cannot occur with certificates issued under this category.

7.3.2.1 MEDIUM (SOFTWARE) - SIGNATURE

This certificate type is a single certificate that may be used to represent a person. Typically this certificate type is referred to as a "Web Browser Certificate". Automated key management cannot occur with this certificate type. This certificate type is most commonly used for SSL with Client Authentication.

7.3.2.2 MEDIUM (HARDWARE) - SIGNATURE

This is a Web certificate type that is stored in hardware, and asserts the "Medium (Hardware)" OID values.

7.3.2.3 DEVICE - WEB SERVER

This certificate type is a single certificate that may be used to represent a Web Server, Database Server, or other device. Automated key management cannot occur with this certificate type. This certificate type is most commonly used for SSL.

7.3.2.4 MEDIUM (SOFTWARE) - CODE SIGN

The Code Signing Certificate type is a single certificate that may be used to digitally sign "mobile code" (ex: Java Applets, and Applications). This certificate normally represents an authoritative entity within an organization whom has the responsibly of performing a "code review" on the "mobile code" source.

7.3.2.5 MEDIUM (HARDWARE) - CODE SIGN

The Code Signing Certificate type is a single certificate that may be used to digitally sign "mobile code" (ex: Java Applets, and Applications). This certificate normally represents an authoritative entity within an organization whom has the responsibly of performing a "code review" on the "mobile code" source.

7.3.2.6 CLIENT SETTING CERTIFICATES

Client Setting Certificates are used to control the behavior of software and toolkits provided by Entrust Technologies. These certificates can cause the client software to operate under specific technical guidelines.

7.3.2.7 ATTRIBUTE CERTIFICATES

Attribute Certificates are certificates that contain authorization data and normally do not contain a public key. These certificates may be used to provide client policy settings enterprise wide, for example, the appropriate symmetric ciphers that may be used by a population of subscribers.

8. Specification Administration

8.1 CHANGE PROCEDURES

The RPS is a document that builds on the CPS. Changes in the RPS that impact CPS procedures and policies have to be submitted through the Treasury CPS Change Procedure.

The following subsections describe the procedure for NASA users to submit/propose changes/updates to the RPS and the Treasury CPS change procedure.

8.1.1 RPS Change Procedures

At the publication of a new RPS, there will be a 15 day period in which comments will be accepted.

Comments on proposed changes must be directed to the NASA PKI Operations. Such communication must include a description of the change, a change justification, contact information for the person requesting the change, and name of the person requesting the change.

At completion of the comment period, the NASA PKI Operations shall review proposed changes for impact to NOCA policies and procedures. The following actions can occur:

- If the proposed change is accepted by the NASA PKI Operations and does not have an impact on CPS procedures and policies. The RPS will be modified and submitted to the Treasury for review.

- If the proposed change is accepted by the NASA PKI Operations and does impact on CPS procedures and policies. The NASA PKI Operations will submit a change request through the Treasury CPS Change Procedure.

- If the proposed change is rejected, the reason will be noted in the disposition of the comments/proposed changes.

8.1.2 CPS Change Procedure

All CPS changes under consideration by the PMO will be disseminated to interested parties. All interested parties may provide their comments to the PMO by submitting in writing comments, applicable CPS sections, and any recommendations for improvement or change. These comments will be either hand-delivered to the PMO or encrypted and signed using at least Medium assurance credentials.

The PMA/PMO will, at a minimum, review the CPS during the Government Fiscal Year 3rd Quarter, taking into consideration any submitted change proposals or recommendations.

CPS changes will also be noted by Change Proposal documents <NOCA CPS Change Proposal YYYY-##> and listed on the change page that precedes the main body of the CPS. The change proposal document will contain the number, reason, date and signature of the person/working group making the change. The original Change Proposal will be signed and then scanned for electronic archiving. In lieu of a hand-written signature, a scanned or typed signature name will be entered for electronic filing.

8.2 PUBLICATION AND NOTIFICATION POLICIES

NASA PKI Operations will publish this RPS on the NASA PKI web site. This RPS is published at URL http://nasaca.nasa.gov. It will also disseminate information via email to any inquiries.

8.3 CPS APPROVAL PROCEDURES

The NASA representative to the Treasury PMA approves this RPS

8.4 WAIVERS

Not applicable.

Appendix A: Acronyms

AES	Advanced Encryption Standard
ARL	Authority Revocation List
BPD	Bureau of Public Debt, US Treasury
CA	Certification Authority
COTR	Contracting Officer's Technical Representative
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DES	Data Encryption Standard
DN	Distinguished Name
DSS	Digital Signature Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
NASA	National Aeronautical and Space Administration
NIST	National Institute of Standards and Technology
OID	Object Identifier
PKCS	Public Key Cryptography Standards
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PA	Policy Authority
RA	Registration Authority
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
SHA	Secure Hash Algorithm
SP	Special Publication
SSL	Secure Sockets Layer
SSP	Shared Service Provider

Appendix B: NASA Identity Verification

PROTECTIVE SERVICES INSTRUCTIONS FOR IDENTITY VERIFICATION

Noted below are the current documented procedures for identity verification performed by the NASA Protective Services. The documents provide a description of the procedures for collecting and verifying identity information per PIV-I.

It should be noted that the procedures described in steps 6 and 7 may change based on the final implementation of the PIV Card Management System.

STEPS FOR PIV CARD ISSSUANCE TO CIVIL SERVANTS

PIV Card Issuance (PCI) Procedures

To obtain and retain certification and accreditation as a Personal Identification Verification (PIV) Card Issuer (PCI) NASA must issue a PIV card with uniformity and common procedures. Adherence to Agency-approved procedures will ensure the proper vetting and credentialing of NASA employees and contractors. It also will garner trust from other government agencies whom we expect to accept the NASA federal credential as an official document that has only been issued upon proper vetting of the credential holder.

FIPS 201 Appendix A graphically displays the following procedure for the issuance of a PIV credential.

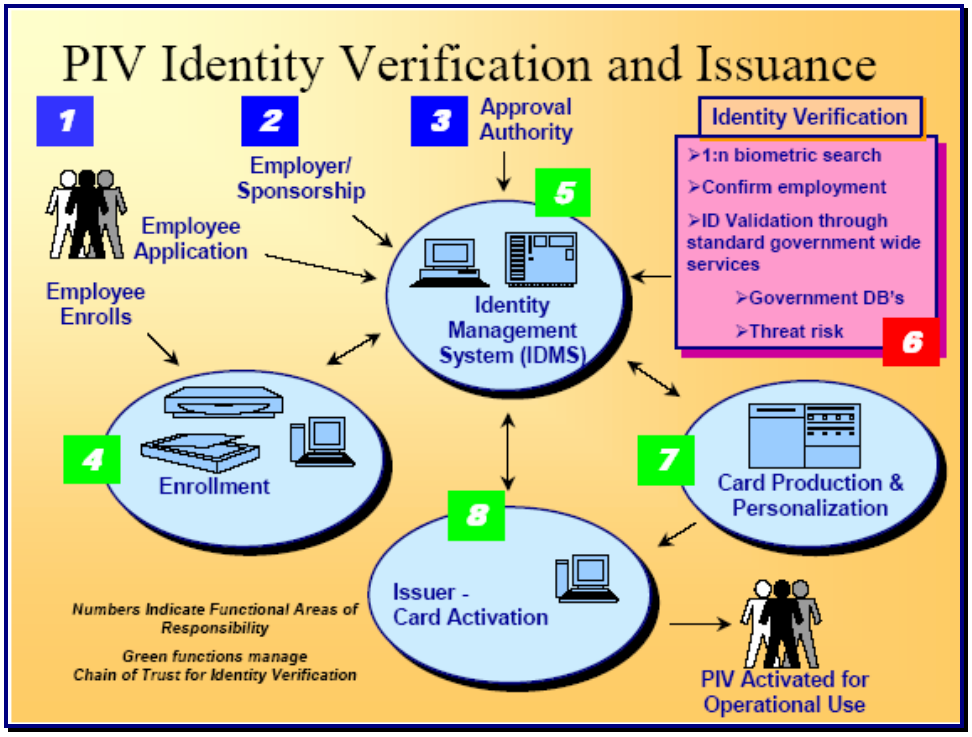


Figure A-1, FIPS 201, Appendix A

The following steps reflect the procedures that a NASA PCI will follow to issue a federal employee a PIV credential:

Step 1:
Human Resources (HR) makes a tentative employment offer to an applicant. The official offer letter shall provide notification of EO 10450 and FIPS 201 requirements for the satisfactory completion of a National Agency Check with Inquiries (NACI) at a minimum. HR's notification shall advise the applicant that an unsatisfactory background investigation could result in withdrawal of the employment offer or immediate termination of employment.

If the applicant is a current Federal employee or has recently separated from another Federal job, HR shall review the OPM databases, and take appropriate steps to validate the applicant's investigation status. Requirements for a NACI or other investigation shall be initiated only if necessary.

Upon acceptance of the employment offer, HR shall provide information to applicants who do not currently possess the required level of background investigation on completing the appropriate security questionnaire form. This information includes instructions on accessing and using e-QIP.

Step 2
Upon acceptance of the employment offer, the applicant is also advised that in order to complete the investigative process, he or she must appear in-person before the authorized PIV registrar and submit two forms of identity source documents in original form. The identity source

documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification, one which must be a Federal[1] or State issued picture identification. Fingerprints are taken at this time. The applicant must appear **no later than** the entry on duty date.

When the applicant appears, the registrar will electronically scan the submitted documents; any document that appears invalid will be rejected by the registrar. The registrar will capture electronically both a facial image and fingerprints of the applicant. The information submitted by the applicant is used to create or update the applicant identity record in the Identity Management System (IDMS).

Step 3:
Upon the applicant's completion of the investigative document, HR reviews and approves the information, resolving discrepancies with the applicant as necessary. When the applicant has appeared in person and completed fingerprints, the package is electronically submitted to initiate the NACI. HR includes a request for feedback on the NAC portion of the NACI at the time the request is submitted.

Step 4:
Prior to entry on duty, HR will make an official request to the Center Chief of Security (CCS) to execute a National Crime Information Center (NCIC) with an Interstate Identification Index check on the applicant. If this process yields negative information, the CCS will immediately notify HR, so that a determination regarding employment may be made.

Step 5:
Upon receipt of the completed NAC, the assigned personnel security specialist will update IDMS from the NAC portion of the NACI and in conjunction with HR indicate the result of the suitability determination.

In compliance with 5CFR732, HR determines employment suitability. If a satisfactory determination is made, the hiring and/or credentialing processes continue. If an unsatisfactory suitability determination is rendered, steps will depend upon the applicant's employment status.

- If the applicant has not yet entered on duty, HR will notify the applicant and the selection official of the decision. All employment processing activities will terminate.

- If the applicant has already entered on duty, appropriate steps will begin to separate the employee.

Based on a favorable NAC and NCIC/III check, the CCS will authorize the issuance of a PIV federal credential in the Physical Access Control System (PACS) database. The CCS, based on information provided by the applicant's supervisor, will determine what physical access the applicant should be granted once the PIV issues the credential.

[1] A non-PIV government identification badge, including the NASA Photo Identification Badge, MAY NOT BE USED for the original issuance of a PIV vetted credential

Although HR renders a suitability determination based on a NAC, the applicant's continued employment is still subject to a favorable adjudication of a completed NACI. If the completed NACI is unfavorably adjudicated, the Center Chief of Security (CCS) will immediately retrieve the employee's PIV card and HR will immediately begin the appropriate separation process.

Step 6:
Using the information provided by the applicant during his or her in-person appearance, the PIV card production facility creates and instantiates the approved PIV card for the employee with an activation date commensurate with employee start date.

Step 7:
The employee proceeds to the credential issuance facility to begin processing for receipt of his/her federal credential.

The employee provides to the credential issuing operator proof of identity with documentation that meets the requirements of FIPS 201 (DHS Employment Eligibility Verification (Form I-9) documents. These documents **must** be the same documents submitted for registration.

The credential issuing operator will verify that the facial image, and optionally reference finger print, matches the enrollment data used to produce the card. Upon verification of identity, the operator will locate the employee's record in the PACS database, and modify the record to indicate the PIV card has been issued. The new employee will select a PIN for use with his or her new PIV card. Although root data is inaccessible to the operator, certain fields (hair color, eye color, et al.) may be modified to more accurately record the employee's information.

The employee proceeds to a kiosk or other workstation to complete activation of the PIV card using the initial PIN entered at card issuance.

PIV CARD ISSUANCE PROCEDURES FOR CONTRACTORS & FOREIGN NATIONALS

PIV Card Issuance (PCI) Procedures

To obtain and retain certification and accreditation as a Personal Identification Verification (PIV) Card Issuer (PCI) NASA must issue a PIV card with uniformity and common procedures. Adherence to Agency-approved procedures will ensure the proper vetting and credentialing of NASA employees, contractors and foreign nationals. It also will garner trust from other government agencies whom we expect to accept the NASA federal credential as an official document that has only been issued upon proper vetting of the credential holder.

FIPS 201 Appendix A graphically displays the following procedure for the issuance of a PIV credential.

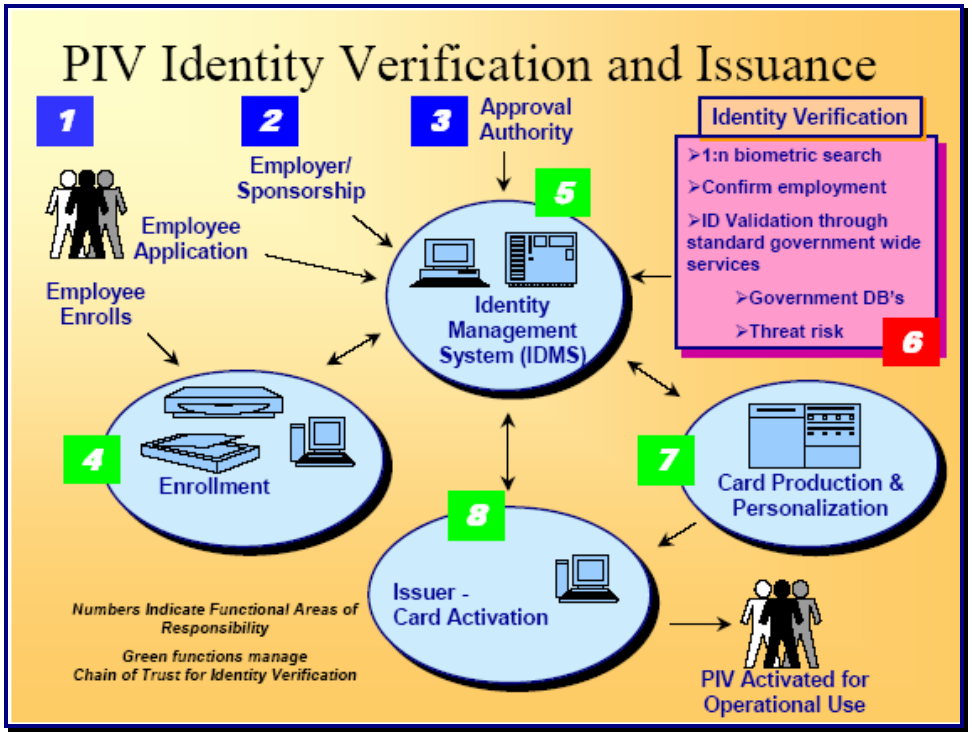


Figure A-1, FIPS 201, Appendix A

The following steps describe the procedures for the NASA Personal Identity Verification Card Issuance (PCI) of a PIV credential:

Step 1:
The Contractor's Corporate Security Officer (CSO), Program Manager (PM), or Facility Security Officer (FSO) submits a formal letter that provides a list of contract employees (applicant) names requesting access to the NASA Contracting Officer's Technical Representative (COTR). In the case of a foreign national applicant, approval through the NASA Foreign National Management System (NFNMS) must be obtained for the visit or assignment before any processing for a PIV credential can take place. Further, if the foreign national is not under a contract where a COTR has been officially designated, the foreign national will provide the information directly to their visit/assignment host, and the host sponsor will fulfill the duties of the COTR mentioned herein. In each case, the letter shall provide notification of the contract or foreign national employee's (hereafter the "applicant") full name (first, middle and last), social security number (SSN) or NASA Foreign National Management System Visitor Number if the foreign national does not have a SSN, and date of birth. If the contract employee has a current satisfactorily completed National Agency Check with Inquiries (NACI) or an equivalent or higher degree of background investigation, the letter shall indicate the type of investigation, the agency completing the investigation, and date the investigation was completed. Also, the letter must specify the risk/sensitivity level associated with the position in which each applicant will be working (NPR 1600.1, §4.5 is germane) Further, the letter shall also acknowledge that contract employees may be denied access to NASA information or information systems based on an unsatisfactory background investigation/adjudication. .

After reviewing the letter for completeness and concurring with the risk/sensitivity levels, the COTR/host must forward the letter to the Center Chief of Security (CCS). The CCS shall review the OPM databases (e.g, DCII, PIP, et al.), and take appropriate steps to validate the applicant's investigation status. Requirements for a NACI or other investigation shall be initiated only if necessary[2].

Applicants who do not currently possess the required level of background investigation shall be directed to the e-QIP web site to complete the necessary background investigation forms online. The CCS shall provide to the COTR/host information and instructions on how to access the e-QIP for each contract or foreign national employee requiring access

Step 2
Upon acceptance of the letter/background information, the applicant will be advised that in order to complete the investigative process, he or she must appear in-person before the authorized PIV registrar and submit two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, Employment Eligibility Verification, one which must be a Federal[3] or State issued picture identification. Fingerprints will be taken at this time. The applicant must appear **no later than** the entry on duty date.

When the applicant appears, the registrar will electronically scan the submitted documents; any document that appears invalid will be rejected by the registrar. The registrar will capture electronically both a facial image and fingerprints of the applicant. The information submitted by the applicant will be used to create or update the applicant identity record in the Identity Management System (IDMS).

Step 3:
Upon the applicant's completion of the investigative document, the CCS reviews the information, and resolves discrepancies with the applicant as necessary. When the applicant has appeared in person and completed fingerprints, the package is electronically submitted to initiate the NACI. The CCS includes a request for feedback on the NAC portion of the NACI at the time the request is submitted.

Step 4
Prior to authorizing physical access of a contractor employee to a federally-controlled facility or access to a Federal information system, the CCS will a National Crime Information Center (NCIC) with an Interstate Identification Index check is/has been performed. In the case of a foreign national, a national check of the Bureau of Immigration and Customs Enforcement (BICE) database will be performed for each applicant. If this process yields negative

[2] At a minimum, a random sampling of reported background investigative information should be made for each contract to provide a level of assurance that investigations were favorably adjudicated.
[3] A non-PIV government identification badge, including the NASA Photo Identification Badge, MAY NOT BE USED for the original issuance of a PIV vetted credential

information, the CCS will immediately notify the COTR/host of the determination regarding access made by the CCS.

Step 5
Upon receipt of the completed NAC, the CCS will update IDMS from the NAC portion of the NACI and indicate the result of the suitability determination. If an unsatisfactory suitability determination is rendered, the COTR will advise the contractor that the employee is being denied physical access to all federally-controlled facilities and Federal information systems.

Based on a favorable NAC and NCIC/III or BICE check, the CCS will authorize the issuance of a PIV federal credential in the Physical Access Control System (PACS) database. The CCS, based on information provided by the COTR/host, will determine what physical access the applicant should be granted once the PIV issues the credential.

Step 6:
Using the information provided by the applicant during his or her in-person appearance, the PIV card production facility creates and instantiates the approved PIV card for the applicant with an activation date commensurate with the applicant's start date.

Step 7:
The applicant proceeds to the credential issuance facility to begin processing for receipt of his/her federal credential.

The applicant provides to the credential issuing operator proof of identity with documentation that meets the requirements of FIPS 201 (DHS Employment Eligibility Verification (Form I-9) documents. These documents **must** be the same documents submitted for registration.

The credential issuing operator will verify that the facial image, and optionally reference finger print, matches the enrollment data used to produce the card. Upon verification of identity, the operator will locate the employee's record in the PACS database, and modify the record to indicate the PIV card has been issued. The applicant will select a PIN for use with his or her new PIV card. Although root data is inaccessible to the operator, certain fields (hair color, eye color, et al.) may be modified to more accurately record the employee's information.

The applicant proceeds to a kiosk or other workstation to complete activation of the PIV card using the initial PIN entered at card issuance.

ALTERNATIVE FOR APPLICANTS WHO DO NOT HAVE A COMPLETED AND ADJUDICATED NAC AT THE TIME OF ENTRANCE ON DUTY

Steps 1 through 4 shall be accomplished for all applicants in accordance with the process described above. If the applicant is unable to appear in person until the time of entry on duty, or does not, for any other reason, have a completed and adjudicated NAC portion of the NACI at the time of entrance on duty, the following interim procedures shall apply.

1. If the documents required to submit the NACI have not been completed prior to EOD, the applicant will be instructed to complete all remaining requirements for submission of the investigation request. This includes presentation of I-9 documents and completion of fingerprints, if not already accomplished. If the applicant fails to complete these activities as prescribed in NPR 1600.1 (Chapters 3 & 4), it may be considered as failure to meet the conditions required for physical access to a federally-controlled facility or access to a Federal information system, and result in denial of such access.

2. Based on favorable results of the NCIC, the applicant shall be issued a temporary NASA identification card for a period not-to-exceed six months. If at the end of the six month period the NAC results have not been returned, the agency will at that time make a determination if an additional extension will be granted for the temporary identification card.

3. Upon return of the completed NAC, the process will continue from Step 5.

ALTERNATIVE FOR APPLICANTS WHO DO NOT HAVE A COMPLETED AND ADJUDICATED NAC AT THE TIME OF ENTRANCE ON DUTY

Steps 1 through 4 shall be accomplished for all employees in accordance with the process described above. If the applicant is unable to appear in person until the time of entry on duty, or does not, for any other reason, have a completed and adjudicated NAC at the time of entrance on duty, the following interim procedures shall apply.

4. If the documents required to submit the NACI have not been completed prior to EOD, the applicant will be instructed to complete all remaining requirements for submission of the investigation request. This includes presentation of I-9 documents and completion of fingerprints, if not already accomplished. If the employee fails to complete these activities as prescribed in NPR 1600.1 (Chapters 3 & 4), it may be considered as failure to meet the conditions of employment, and result in termination.

5. Based on favorable results of the NCIC, the applicant shall be issued a temporary NASA identification card for a period not-to-exceed six months. If at the end of the six month period the NACI results have not been returned, the agency will at that time make a determination if an additional extension will be granted for the temporary identification card.

6. Upon return of the completed NAC, the process will continue from Step 5.

APPENDIX C: NASA PIV-I AND NOCA CPS Identity Verification Processes

Below is a cross reference between the NOCA CPS identity authentication requirements and the NASA PIV-I processes. In regards to the NOCA CPS in-person proofing processes.

CROSS-REFERENCE OF NOCA CPS REQUIREMENTS AND NASA IDENTITY PROOFING

NOCA CPS Requirement Section Text	NASA
NASA EMPLOYEES - CIVIL SERVANTS	
Section 3.1.9 - item #1 Verify that a request for certificate issuance to the applicant was submitted by agency management	The PIV Request process is used to initiate request for certificates. In the case of personnel not yet issued a PIV card, a separate request.
Section 3.1.9 - item #2 Applicant's employment will be verified through use of official agency records.	NASA IdMAX system will have information on applicants. If applicant is a civil servant, IdMAX will have information from the Federal HR system.
Section 3.1.9 - Process #1 - -item a) i The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity,	For PIV and non-PIV issuance, applicants must present two identity documents from the I-9 list for identity verification by NASA Protective Services.
Section 3.1.9 - Process #1 - -item a) ii The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant)	For PIV card issuance this will be done before card and credential are issued For non-PIV personnel this will be performed at time of activation code issuance.
Section 3.1.9 - Process #1 - -item a) iii The credential presented in step a) ii above will be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.	Applicants must provide 2 documents from the I-9 list. Protective Services keeps a copy for identity proofing and scans the documents. Any concerns about document legitimacy will be surfaced during the NACI investigation.
Section 3.1.9 - item #4 A biometric of the applicant (e.g., a photograph or fingerprint) will be recorded and maintained by the RA or CA. (Handwritten signatures and other	For personnel issued PIV cards, a biometric is recorded by NASA protective services both picture and fingerprint.

behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.	
CONTRACTORS AND OTHER AFFILIATED PERSONNEL	
Section 3.1.9 - item #1 [Contractors] Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative);	The PIV Request process is used to initiate request for certificates. For contractors a COTR is identified. In the case of non-PIV personnel, a separate request will be provided that must be signed by the requestors sponsor.
Section 3.1.9 - item #2 [Contractors] Sponsoring Agency employee's identity and employment will be verified through either of the following methods: a.) A digital signature verified by a currently valid employee signature certificate issued by the CA, may be accepted as proof of both employment and identity, Or b.) Employee's identity will be established by in-person proofing before the Registration Authority as in employee authentication above and employment validated through use of the official agency records.	For Contractors being issued PIV credentials, contractor's identity is verified as part of the PIV-1 process. In the case of non-PIV contact personnel, a separate request will be provided that must be signed by the requestors sponsor. The request can be digitally signed or sent as an attachment in digitally signed email.
Section 3.1.9 - Process #1 - -item a) i [Contractors] The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity,	Onsite contractors will have already submitted two documents to protective services for identity proofing.
Section 3.1.9 - Process #1 - -item a) ii [Contractors] The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant)	For PIV card issuance this will be done before card and credential are issued For non-PIV personnel this will be performed at time of activation code issuance.
Section 3.1.9 - Process #1 - -item a) iii [Contractors] The credential presented in step a) ii above will be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential.	As part of the PIV-I identity proofing, personnel requesting badges must provide 2 documents from the I-9 list. Protective Services keeps a copy for identity proofing any concerns about document legitimacy will be surfaced during the NACI investigation

Section 3.1.9 - item #4 [Contractors] A biometric of the applicant (e.g., a photograph or fingerprint) will be recorded and maintained by the RA or CA.	For personnel issued PIV cards, a biometric is recorded by NASA protective services both picture and fingerprint.
Identity Proofing Documentation	
Section 3.1.9 Additionally, the RA will record the process that was followed for issuance of each certificate. The process documentation and authentication requirements will include	
The identity of the person performing the identification;	This is done by OPM and FBI for PIV
A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);	Identity verification is done through Federal systems, OPM and FBI. These systems would have this information.
Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);	Documents are copied or scanned by Protective Services.
The biometric of the applicant;	Captured by Protective Services
The date and time of the verification	IdMax will have information on receipt of ID vetting results.
A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).	As applicants input identity information in the OPM e-QIP system. Any identity declarations are captured in e-QIP.

APPENDIX D: Unsworn Declaration

From the U.S. Code Online via GPO Access
[wais.access.gpo.gov]
[Laws in effect as of January 20, 2004]
[Document not affected by Public Laws enacted between
January 20, 2004 and December 23, 2004]
[CITE: **28USC1746**]

TITLE 28--JUDICIARY AND JUDICIAL PROCEDURE

PART V--PROCEDURE

CHAPTER 115--EVIDENCE; DOCUMENTARY

Sec. 1746. Unsworn declarations under penalty of perjury

Wherever, under any law of the United States or under any rule, regulation, order, or requirement made pursuant to law, any matter is required or permitted to be supported, evidenced, established, or proved by the sworn declaration, verification, certificate, statement, oath, or affidavit, in writing of the person making the same (other than a deposition, or an oath of office, or an oath required to be taken before a specified official other than a notary public), such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration, certificate, verification, or statement, in writing of such person which is subscribed by him, as true under penalty of perjury, and dated, in substantially the following form:

(1) If executed without the United States: ``I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date).

(Signature)''.

(2) If executed within the United States, its territories, possessions, or commonwealths: ``I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date).

(Signature)''.

(Added Pub. L. 94-550, Sec. 1(a), Oct. 18, 1976, 90 Stat. 2534.)

Prior Provisions

A prior section 1746 was renumbered section 1745 of this title.

APPENDIX E: Definitions

Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Assurance	How well a Relying Party can be certain of or trust the certificate. The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on multiple factors that include the proper registration of Subscribers, the proper generation and management of the certificate and associated private keys, in accordance with the stipulations of the CP. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates
Authority Revocation List (ARL)	A list of revoked CA certificates. An ARL is a CRL for CA cross certificates.
CA Public Key	The public key portion of the CA signing key pair, which is used to verify certificates, certificate revocation lists and authority revocation lists signed by the CA signing key.
Certificate	The public key of a user, together with some other information, rendered unforgeable by digitally signing it with the private key of the certification authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509.
Certificate Policy (CP)	A document that defines the policies of a Certificate Authority (CA). A CP addresses all aspects associated with generation, production, distribution, recovery and administration of digital certificates. A CP also defines the policies for administration and operation of a CA.
Certification Practice Statement (CPS)	A statement of practices that a CA employs to implement the specific policies defined in the Certification Policy (CP).
Certificate Revocation List (CRL)	A list of revoked certificates that is created and signed by the same CA that issued the certificates. A certificate is added to the list if it is revoked (e.g., because of suspected

	key compromise). In some circumstances the CA may choose to split a CRL into a series of smaller CRLs.
Certification Authority	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Cross-certification	The process of establishing a trust relationship between two Certification Authorities. A process by which two Certification Authorities (CAs) securely exchange keying information so that each can certify the trustworthiness of the other's keys. Once the CAs has cross-certified, users within the CA domains can validate each other's certificates.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine: (a) whether the transformation was created using the key that corresponds to the signer's key; and (b) whether the message has been altered since the transformation was made.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Employee	An employee is any person employed by NASA.
End Entity	An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End Entity may be a Subscriber, a Relying Party, a device, or an application.
Entity	Any autonomous element within the Public Key Infrastructure. This may be a CA, a RA or an End Entity.
Key	In cryptography, a secret value that is used in an encryption algorithm to encrypt and decrypt data.
Key Pair	Two mathematically related keys having the following properties: 1.) one key can be used to encrypt a message that can only be decrypted using the other key 2.) knowing one key, it is computationally infeasible to discover the other key.
Object Identifier	(OID) The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

Organization	A department, agency, corporation, partnership, trust, joint venture or other association.
Policy Authority	A body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs.
Public Key	The portion of the public key pair that is available to everyone. The public key is stored in the directory. The NASA PKI uses a public key for encryption and a public (i.e. verification) key for verifying a digital signature.
Public Key Cryptography	Public key cryptography is a cryptographic system that uses key pairs. One key of the pair is public and the other key is private and known only to the owner. The mathematical relationship between the keys is such that an action performed by one key (i.e. encryption) can be undone by the other key (i.e. decryption). In addition, the relationship between the keys is such that knowing the public key does not compromise the private key. The NASA PKI uses two key pairs, one pair for encryption and one pair for signing.
Public Key Cryptography Standards	The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. PKCS documents have become widely referenced and implemented.
Public Key Cryptography Standards #12	This standard specifies a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc.
Public Key Infrastructure	A structure of hardware, software, people, processes and policies that uses Digital Signature technology to provide Relying Parties with a verifiable association between the public component of an asymmetric key pair with a specific Subscriber.
Private Key	The portion of the public key pair that is kept secret by the owner of the key pair. The NASA PKI uses a private key for encryption and a private signing key for digital signatures.
Reason Code	A code put in the certificate to indicate the reason why the certificate was revoked.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of certificate Subscribers before certificate

	issuance, but does not actually sign the certificates (i.e., a RA is delegated certain tasks on behalf of a CA).
Relying Party	A person who uses a certificate signed by a CA to authenticate a digital signature or to encrypt communications to the certificate subject, and is a Subscriber of the CA or a PKI which is cross certified with the CA.
Sensitive Unclassified	Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.
Sponsor	A Sponsor in the NASA PKI is the NASA department or civil servant that has nominated that a specific individual or organization be issued a certificate. (E.g., for an employee this may be the employee's manager). The Sponsor is responsible for informing the CA or RA if the relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.
Subscriber	An individual or organization whose public key is certified in a public key certificate. In the NASA PKI this could be a civil servant, or a NASA contractor. Subscribers may have one or more certificates from a specific CA associated with them; most will have at least two active certificates - one containing their Digital Signature key; the other containing their Confidentiality (I.E. encryption) key.

REFERENCES

The documents noted below were referenced in the RPS.

CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf
COMMON	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, November 1, 2004 http://www.cio.gov/ficc/documents/CommonPolicy.pdf.
FIPS 112	Password Usage, 1985-05-30 http://csrc.nist.gov/publications/fips/fips112/fip112-1.pdf http://csrc.nist.gov/publications/fips/fips112/fip112-2.pdf
FIPS 140-1	Security Requirements for Cryptographic Modules, 1994-01 http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
FIPS 140-2	Security Requirements for Cryptographic Modules, 2001-06 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 186-2	Digital Signature Standard (DSS), FIPS 186-2, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf
FIPS 201	Personal Identity Verification (PIV) of Federal Employees and Contractors http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
PACS	Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004.
PKCS#1	Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003.
PKCS#11	Cryptographic Token Interface Standard, Version 2.01 ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/201final/spec/v201.pdf
PKCS#12	Personal Information Exchange Syntax Standard, Version 1.0 ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RFC-2510	Certificate Management Protocols, Adams and Farrell, March 1999 ftp://ftp.rfc-editor.org/in-notes/rfc2510.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. ftp://ftp.rfc-editor.org/in-notes/rfc2560.txt
SSP Agency CA CPS	Department of Treasury Public Key Infrastructure, SSP Agency CA Certification Practice Statement, May 17, 2006, version 1.4.
USGold	GOVERNMENTWIDE DIRECTORY SUPPORT 2 TECHNICAL SERIES: The Updated USGold Schema, July 14, 1997. http://csrc.nist.gov/pki/twg/directory_references.htm